H3C SecPath ACG1000 系列应用控制网关

Web 配置指导

新华三技术有限公司
http://www.h3c.com
资料版本：6W106-20220607

Copyright © 2020-2022 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其它原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

本配置指导主要介绍了 H3C SecPath ACG1000 系列应用控制网关的 Web 页面和配置方法。

前言部分包含如下内容：

- 读者对象
- 本书约定
- 资料意见反馈

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其它运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 Web 管理概述 ····· 1-1
1.1 简介 ····· 1-1
1.2 设备默认配置 ····· 1-1
1.2.1 管理口的默认配置 ····· 1-1
1.2.2 默认管理员用户 ····· 1-1
1.3 WEB 界面布局描述 ····· 1-1
1.4 列表 ····· 1-1
1.5 图标 ····· 1-2

1 Web 管理概述

1.1 简介

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，便能够配置并管理设备。在进行 Web 管理前，必须配置设备使其能够接受来自指定接口的 HTTP 或 HTTPS 管理。

注意

推荐使用 IE11.0 及以上版本或 Google Chrome 69 及以上版本、 Firefox71.0 及以上版本浏览器对设备进行 WEB 管理，最佳显示分辨率为 1366 × 768。如使用其它版本浏览器可能出现显示上兼容性不佳的情况，请用户知晓。

1.2 设备默认配置

1.2.1 管理口的默认配置

管理口的默认地址配置为 192.168.1.1/24。默认允许对该接口进行 PING，HTTPS 操作。

1.2.2 默认管理员用户

系统默认的管理员用户为 admin，默认密码为 admin。用户可以使用这个管理员账号从任何可访问设备的地址登录设备，并且使用设备的所有功能；首次登录设备时，系统会强制修改密码。

1.3 WEB界面布局描述

Web 管理界面由菜单、标签栏和页面组成，每个菜单有相应的多个标签栏，每个标签有相关的页面。当您点击一个菜单项目，如系统管理，系统菜单会扩展为一个子菜单。接着点击其中一个子菜单后，相关联的页面会在其对应的标签栏中显示。点击标签栏查看不同的页面内容。

1.4 列表

很多管理配置页面都是以列表的形式呈现，例如管理员、接口、安全策略等，如下图 1-1：

图1-1 列表

列表中的条目显示各项信息。列表中最右面的列一般为图标按钮列，可对该条目进行一些操作，例如编辑、删除等。

通过列表上方的<新建>按钮，可以增加条目。<新建>按钮切换到对话框形式的页面，新建和编辑操作的页面是基本一致的。

1.5 图标

页面中有很多图标可以帮助各功能项进行配置管理操作，表 1-1 对页面中的图标进行说明。

表1-1 图标

图标	名称	说明
	新建	新建条目
	删除	删除选中条目
	启用过滤器	过滤符合条件的条目
	编辑/删除	编辑配置
	启用	启用选中条目
	禁用	禁用选中条目
	刷新	刷新当前页面或图表
	冻结	冻结选中用户
	导入	从本地导入配置版本文件/特征库文件到设备
	导出	从设备导出配置到本地
	提交	提交当前页面的配置内容
	取消	取消当前页面的配置内容

目 录

1 主页……1-1
1.1 主页简介……1-1
1.2 主页布局设置……1-1
1.3 主页展示信息……1-2
1.3.1 行为管理……1-2
1.3.2 系统信息……1-3
1.3.3 系统资源……1-5
1.3.4 实时流量图……1-6
1.3.5 接口状态……1-7
1.3.6 用户流量……1-7
1.3.7 应用流量……1-9
1.3.8 系统日志……1-11
1.3.9 审计日志……1-12
1.3.10 入侵防御……1-12
1.3.11 攻击趋势……1-14
1.3.12 威胁日志……1-14
1.3.13 会话数……1-15

1 主页

1.1 主页简介

主页主要包含了系统当前的状态信息，包括以下信息：

- 行为管理：展示在线用户、审计日志、流量分析及违规用户信息。
- 系统信息：展示设备信息、HA 状态信息及授权信息等。
- 系统资源：展示 cpu、内存及磁盘信息。
- 实时流量：展示系统最近一个小时的流量统计信息。
- 接口状态：展示物理接口的状态信息。
- 用户流量：展示用户流量排行信息。
- 应用流量：展示应用流量排行信息。
- 系统日志：主要显示系统日志信息。
- 审计日志：显示 IM 聊天、邮件收发、文件传输、搜索引擎等上网行为审计信息。

用户登录到 Web 后，默认进入“主页”页面。

1.2 主页布局设置

进入“主页”页面，点击右上角的“设置”按钮，弹出页面布局设定窗口，可以自定义主页显示的窗口模块，设置完成后点击“保存风格”保存设置。勾选的模块会在页面显示，如下图所示。

图1-1 主页设置

点击“恢复默认”按钮，弹出的提示确认窗口，点击“确认”后恢复默认设置，默认显示的模块如下图所示。

图1-2 页面布局设定恢复默认

1.3 主页展示信息

1.3.1 行为管理

在导航栏中选择“主页”，可以看到“行为管理”标签，如图 1-3 所示。

图1-3 行为管理

对于行为管理信息的详细说明如表 1-2 所示。

表1-1 系统信息说明

标题项	说明
在线用户	统计设备在线用户总数，点击总数可跳转到在线用户页面。
认证用户	统计设备认证用户总数。
匿名用户	统计设备匿名用户总数。
审计日志	统计当天审计日志总数。
IM聊天	统计当天IM聊天日志总数，点击总数可以展示IM聊天日志详细。
社区论坛	统计当天社区论坛日志总数，点击总数可以展示社区论坛日志详细。
引擎搜索	统计当天引擎搜索日志总数，点击总数可以展示引擎搜索日志详细。

标题项	说明
网站访问	统计当天网站访问日志总数，点击总数可以展示网站访问日志详细。
邮件收发	统计当天邮件收发日志总数，点击总数可以展示邮件收发日志详细。
文件传输	统计当天文件传输日志总数，点击总数可以展示文件传输日志详细。
娱乐股票	统计当天娱乐股票日志总数，点击总数可以展示娱乐股票日志详细。
其它	显示当天其它日志总数，点击总数可以展示其它日志详细。
流量分析	显示线路质量评分等级，有三个等级：优、良、差，点击评分等级可以展示流量监控信息。
线路名	线路名称。
线路带宽	线路设置带宽。
实时流量	线路实时流量统计。
违规用户数	统计当天的阻断用户总数。
策略违规用户	统计当天的应用控制策略违规用户总数，点击总数可以展示应用控制阻断日志。
共享终端违规用户	统计当天的共享终端违规用户总数，点击总数可以展示共享终端监控页面。
限额违规用户	统计当天的用户限额违规用户总数，点击总数可以展示限额用户统计页面。

说明

流量分析展示需要配置流控策略，才可显示流量分析数据。

1.3.2 系统信息

在导航栏中选择“主页”，可以看到“系统信息”标签，如图 1-4 所示。

图1-4 系统信息

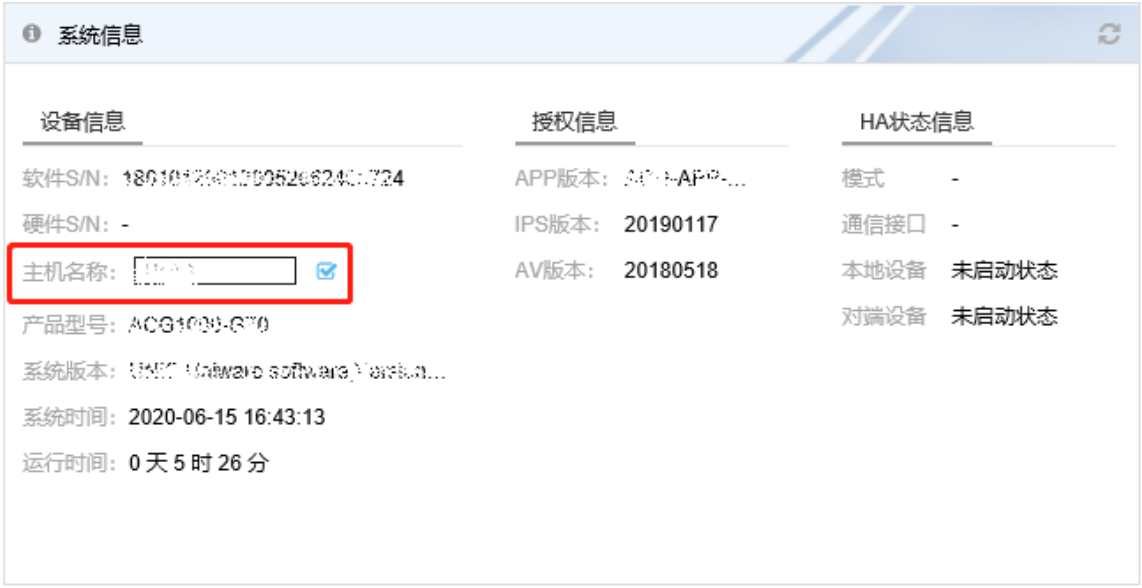
对系统信息的详细说明如表 1-2 所示。

表1-2 系统信息说明

标题项	说明
软件S/N	设备软件的唯一标识，是设备出厂时设定好的。
硬件S/N	设备硬件的唯一标识，是设备出厂时设定好的。
主机名称	通过主机名称区分设备。
产品型号	产品的型号。
系统版本	当前设备运行的系统软件的版本号。
系统时间	表示系统当前时间。
运行时间	表示系统从上次启动已经运行的时间。
APP版本	应用控制特征库版本信息。
IPS版本	应用控制特征库版本信息。
AV版本	病毒防护特征库版本信息。
模式	HA的模式。
通信接口	HA的心跳接口。
本地设备	本地设备的HA状态。
对端设备	对端设备的HA状态。

点击<编辑>按钮可修改当前管理设备的主机名，便于用户区分不同设备。如图 1-5 所示，点击该按钮可弹出修改对话框，填写自定义主机名后点击<保存>即可生效。

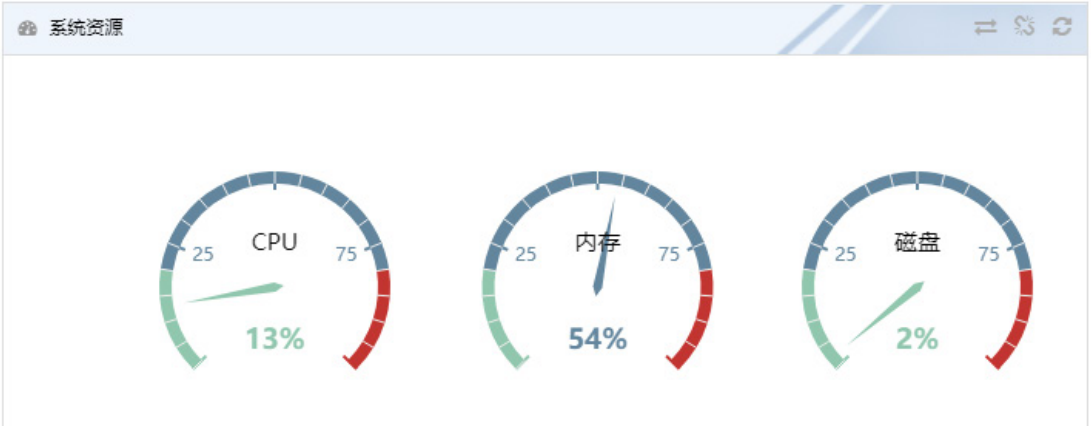
图1-5 编辑主机名称



1.3.3 系统资源

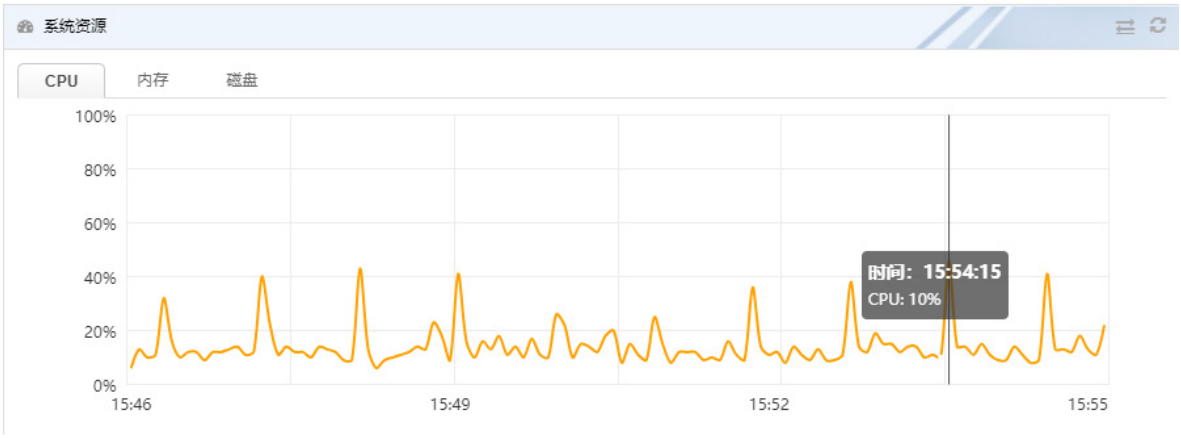
在导航栏中选择“主页>主页”，可以看到“系统资源”标签，如图 1-6 所示。

图1-6 系统资源



点击右上角的转换按钮，切换为曲线图形式，可显示最近 10 分钟的系统资源情况，如图 1-7 所示。

图1-7 系统资源曲线图



对系统资源的详细说明如表 1-3 所示：

表1-3 系统资源说明

标题项	说明
CPU	处理器的利用率，是系统所有处理器最近一分钟内的平均值。
MEM	系统内存利用率，此内存利用率为整个系统的内存利用率。
磁盘	系统的磁盘利用率。

点击右上角<刷新>按钮可以立即刷新当前的显示。

1.3.4 实时流量图

在导航栏中选择“主页>主页”，可以看到“实时流量图”标签，如图 1-8 所示。

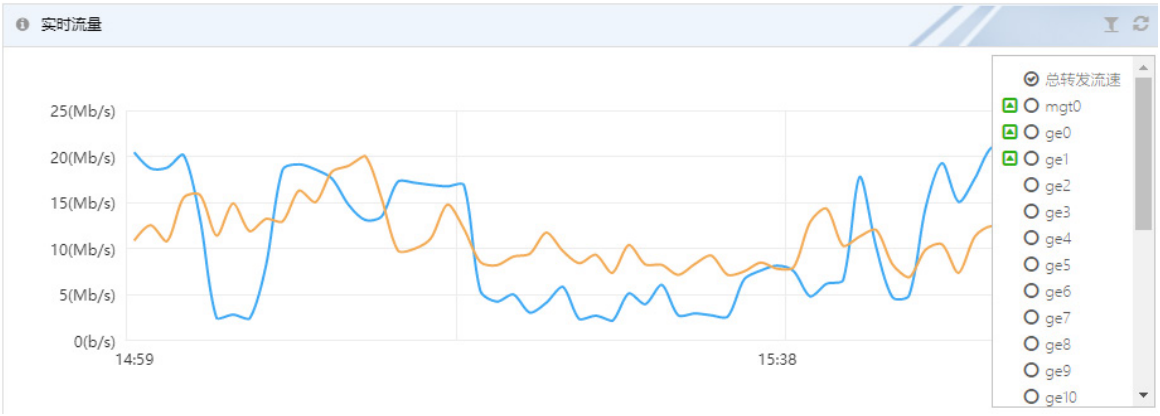
图1-8 实时流量图

该面板可显示当前系统最近一小时整机的吞吐量曲线图，根据该曲线图可查看系统最近一个小时的流量情况，从而判断实际网络使用情况。

当用户打开管理界面首页时，系统每隔 15 秒会自动刷新实时流量统计图表。

点击右上角的<编辑>按钮，如图 1-9 所示，可以编辑流量图显示的选项。

图1-9 编辑流量图显示



点击右上角<刷新>按钮可以立即刷新当前的显示。

1.3.5 接口状态

在导航栏中选择“主页”，可以看到“接口状态”标签，如图 1-10 所示。

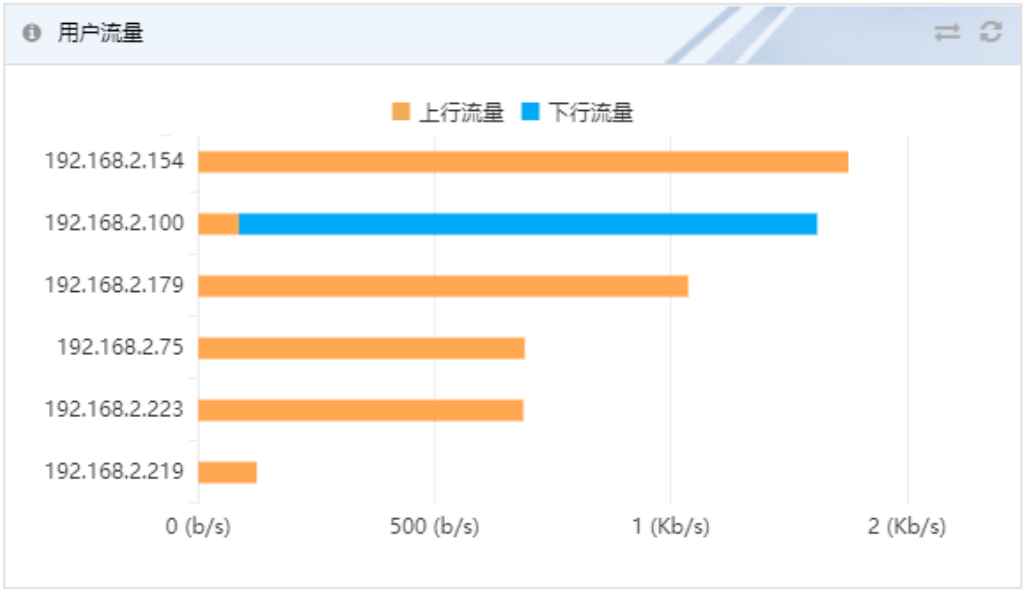
图1-10 接口状态

该面板能够显示设备真实物理接口状态：链路开启状态、IP 地址、双工状态、工作模式以及收发包速率，当前在线的接口显示为绿色，没有插上网线或者物理状态为 DOWN 的接口则显示为灰色。

1.3.6 用户流量

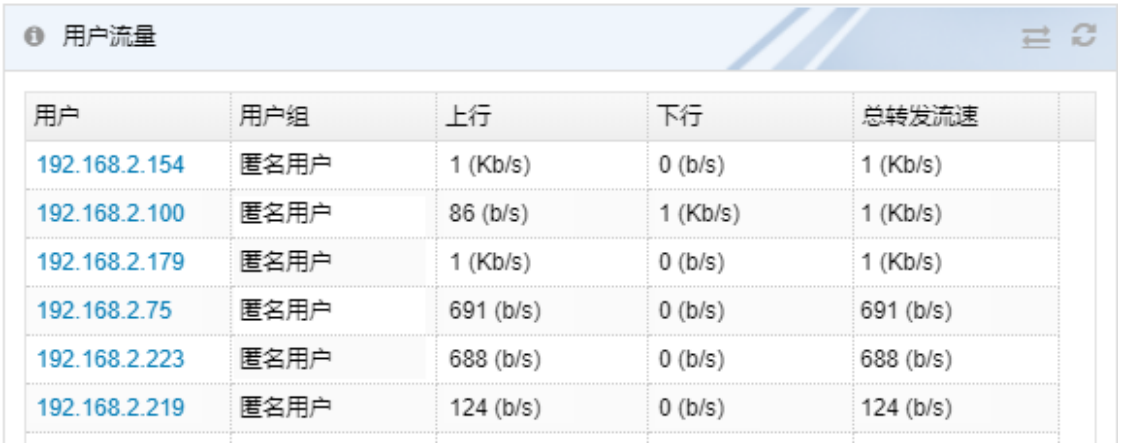
在导航栏中选择“主页>主页”，可以看到“用户流量”标签，如图 1-11 所示。

图1-11 用户流量



点击右上角的转换按钮，可切换为列表形式，如图 1-12 所示。

图1-12 用户流量列表



用户	用户组	上行	下行	总转发流速
192.168.2.154	匿名用户	1 (Kb/s)	0 (b/s)	1 (Kb/s)
192.168.2.100	匿名用户	86 (b/s)	1 (Kb/s)	1 (Kb/s)
192.168.2.179	匿名用户	1 (Kb/s)	0 (b/s)	1 (Kb/s)
192.168.2.75	匿名用户	691 (b/s)	0 (b/s)	691 (b/s)
192.168.2.223	匿名用户	688 (b/s)	0 (b/s)	688 (b/s)
192.168.2.219	匿名用户	124 (b/s)	0 (b/s)	124 (b/s)

对用户流量的详细说明如表 1-4 所示。

表1-4 用户流量说明

标题项	说明
用户	通过设备上网的用户，可为绑定IP的用户，也可为认证用户。
用户组	通过设备上网的用户所属的用户组。
上行	显示该用户当前上行流速大小。
下行	显示该用户当前下行流速大小。
总流速	显示该用户当前上下行总流速大小。

点击右上角<刷新>按钮可以立即刷新当前的显示。

点击具体用户名，如图 1-13 所示，可查看该用户流量详细信息，包括用户会话、用户实时流速、应用统计详细信息。

图1-13 用户流量详细信息

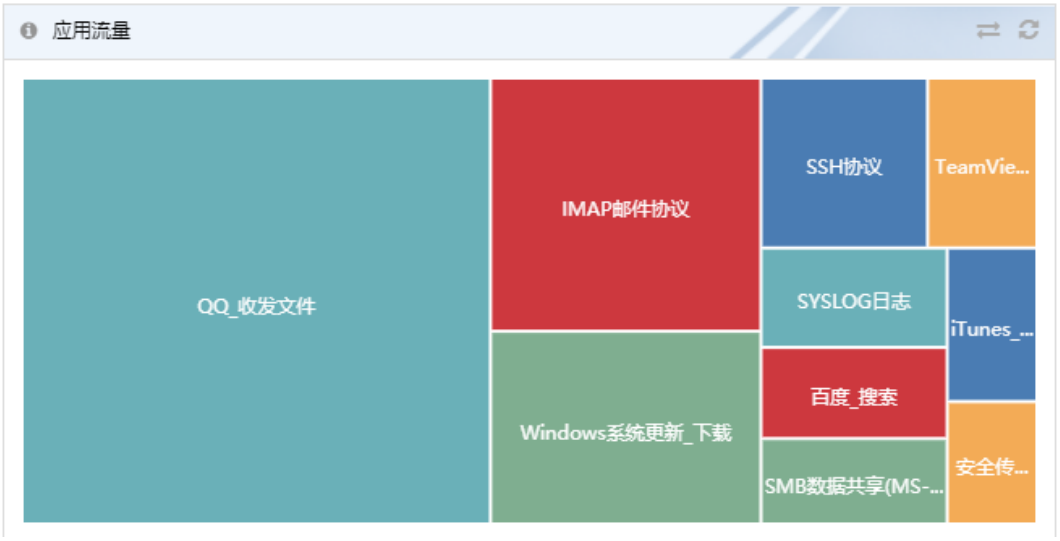
应用统计详细信息

	应用名	上行速率	下行速率	总速率	当前会话数
1	其他TCP	3.50(Kb/s)	29.84(Kb/s)	33.34(Kb/s)	2

1.3.7 应用流量

在导航栏中选择“主页”，可以看到“应用流量”标签，如图 1-14 所示。

图1-14 应用流量



点击右上角的转换按钮，可切换为列表形式，如图 1-12 所示。

图1-15 应用流量排名列表

对应用流量的详细说明如表 1-5 所示。

表1-5 应用流量排名说明

标题项	说明
应用类型	列举当前总流速排名前十的应用名称。
上行	显示该应用当前上行流速大小。
下行	显示该应用当前下行流速大小。
总流速	显示该应用当前上下行总流速大小。
百分比	显示该应用当前总流速占整体流速的百分比。

点击右上角<刷新>按钮可以立即刷新当前的显示。

点击应用名称，如图 1-16 所示，可查看该应用流量下排名前五的用户，并显示用户名、上行、下行和总流速。

图1-16 应用流量详细信息

1.3.8 系统日志

在导航栏中选择“主页”，可以看到“系统日志”标签，如图 1-17 所示。

图1-17 系统日志

对系统日志的详细说明如表 1-6 所示。

表1-6 系统日志说明

标题项	说明
日志内容	日志的详细说明内容
时间	日志产生时间

点击右上角<刷新>按钮可以立即刷新当前的显示。

1.3.9 审计日志

在导航栏中选择“主页”，可以看到“审计日志”标签，审计日志包括 IM 聊天日志、邮件收发日志、文件传输日志和搜索引擎日志。如图 1-18 所示。

图1-18 审计日志

对审计日志的详细说明如表 1-7 所示。

表1-7 审计日志说明

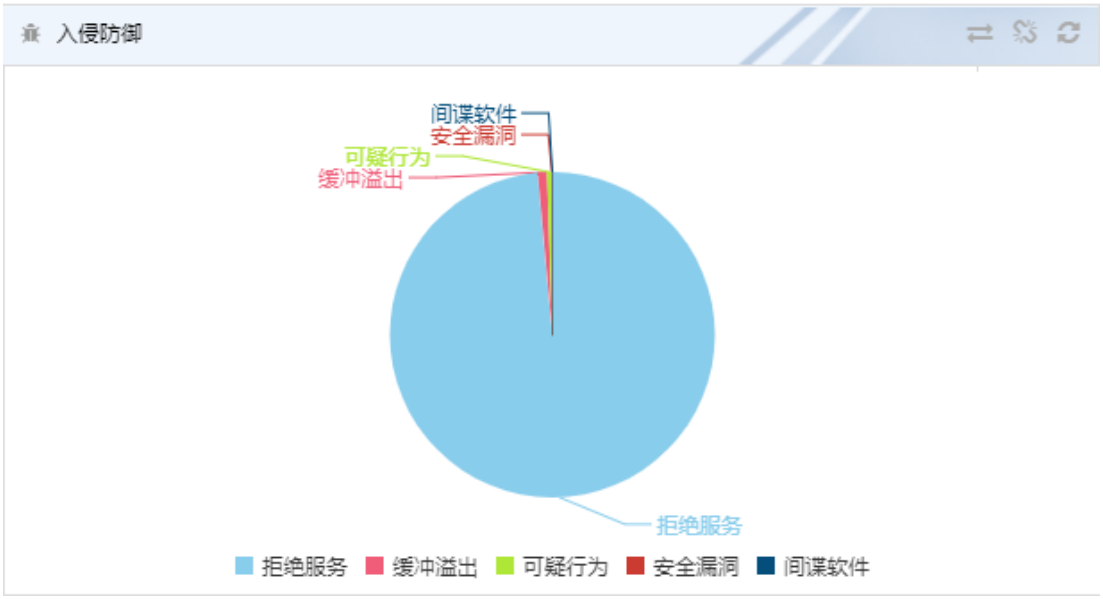
标题项	说明
用户	审计的用户
应用	审计的应用
行为	审计的行为
内容	审计的搜索内容

点击右上角<刷新>按钮可以立即刷新当前的显示。

1.3.10 入侵防御

在导航栏中选择“主页”，可以看到“入侵防御”标签，如图 1-19 所示。该面板以饼图的形式展示当前系统最近一天的入侵防御事件类型占比，从而帮助管理员判断实际网络安全情况。

图1-19 入侵防御



点击右上角的转换按钮，可切换为列表形式，如图 1-20 所示。

图1-20 入侵防御列表

威胁类型	威胁数量	占比
拒绝服务	12795	98.57%
缓冲溢出	117	0.9%
可疑行为	59	0.45%
安全漏洞	8	0.06%
间谍软件	2	0.02%

对入侵防御的详细说明如表 1-8 所示。

表1-8 用户流量说明

标题项	说明
威胁类型	显示入侵防御各事件类型。
威胁数量	显示入侵防御各事件类型的威胁数量。
占比	显示入侵防御各事件类型的占比。

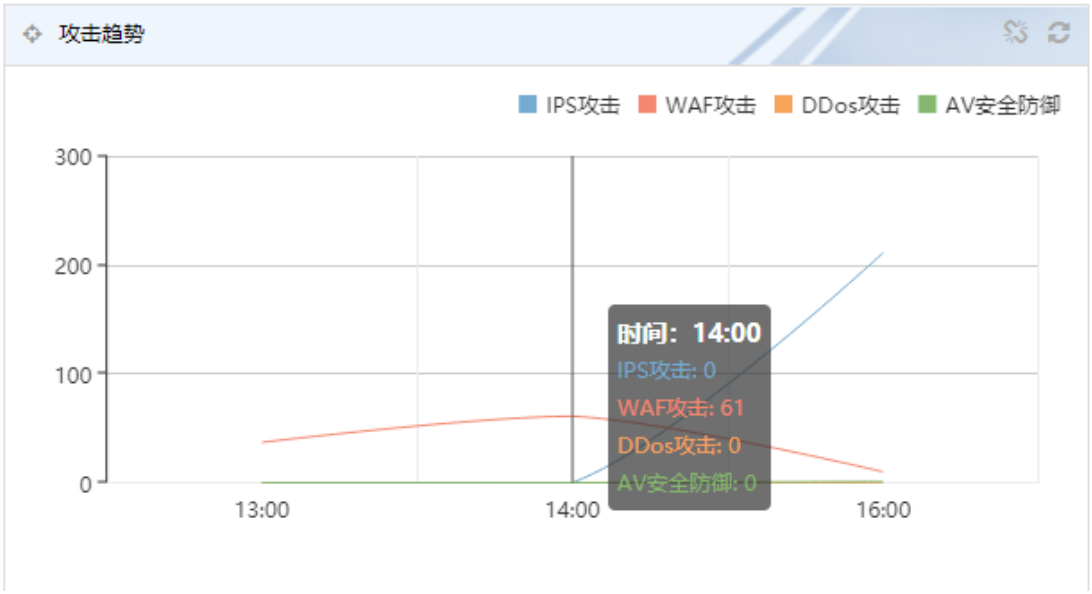
点击右上角按钮，可以设置显示信息的自动刷新时间，默认系统会每隔 30 秒自动刷新显示信息。

点击右上角刷新按钮，可以立即刷新当前的显示。

1.3.11 攻击趋势

在导航栏中选择“主页”，可以看到“攻击趋势”标签，如图 1-21 所示。该面板可显示当前系统最近一天的网络攻击趋势图，包括 IPS 攻击、WAF 攻击、Ddos 攻击及 AV 安全防御的趋势曲线。

图1-21 攻击趋势



将鼠标放在曲线图上，将显示该时间点的攻击次数。

点击右上角按钮，可以设置显示信息的自动刷新时间，默认系统会每隔 30 秒自动刷新显示信息。

点击右上角刷新按钮，可以立即刷新当前的显示。

1.3.12 威胁日志

在导航栏中选择“主页”，可以看到“审计日志”标签，如图 1-22 所示。该面板可展示最近 20 条的入侵检测、病毒防护、安全防护日志，其中入侵检测、病毒防护只报级别为警告及以上的最近 20 条日志。

图1-22 威胁日志

点击右上角按钮，可以设置显示信息的自动刷新时间，默认系统会每隔 30 秒自动刷新显示信息。

点击右上角刷新按钮，可以立即刷新当前的显示。

1.3.13 会话数

在导航栏中选择“主页”，可以看到“会话数”标签，如图 1-23 所示。该面板可展示最近 10 分钟的当前会话数和新增会话数趋势图，从而判断实际网络情况。

图1-23 会话数

将鼠标放在曲线图上，将显示该时间点的新增会话数及当前会话数。

点击右上角 按钮，可以设置显示信息的自动刷新时间，默认系统会每隔 30 秒自动刷新显示信息。

点击右上角刷新按钮 ，可以立即刷新当前的显示。

目 录

1 系统监控 ····· 1-1
1.1 在线用户管理 ····· 1-1
1.2 接口状态 ····· 1-2
1.3 黑名单记录 ····· 1-4
1.3.1 黑名单概述 ····· 1-4
1.3.2 黑名单添加 ····· 1-4
1.3.3 黑名单编辑 ····· 1-5
1.3.4 黑名单删除 ····· 1-5
1.3.5 黑名单记录 ····· 1-6
1.3.6 黑名单配置举例 ····· 1-6
1.4 SSL VPN 在线用户管理 ····· 1-7
1.5 实时流速监控 ····· 1-8
1.5.1 用户实时流速 ····· 1-8
1.5.2 应用实时流速 ····· 1-9
1.6 资产管理 ····· 1-12
1.6.1 资产管理概述 ····· 1-12
1.6.2 资产管理配置 ····· 1-12
1.6.3 资产识别设定 ····· 1-14
1.6.4 资产识别配置举例 ····· 1-16
1.7 故障监控中心 ····· 1-19
1.7.1 简介 ····· 1-19
1.7.2 单用户检测配置 ····· 1-19
1.7.3 单用户检测配置举例 ····· 1-22
2 数据分析 ····· 2-25
2.1 数据分析简介 ····· 2-25
2.2 用户流量统计 ····· 2-25
2.3 应用流量统计 ····· 2-27
2.4 用户信息中心 ····· 2-30
2.4.1 虚拟用户身份 ····· 2-31
2.4.2 用户日志统计 ····· 2-32
2.4.3 应用流量比例 ····· 2-33
2.4.4 用户-访问网站分析 ····· 2-34

2.4.5 用户轨迹时光轴 ····· 2-35
2.5 设备流量统计 ····· 2-35
2.6 设备健康统计 ····· 2-36
2.7 会话监控统计 ····· 2-40
2.7.1 会话统计 ····· 2-40
2.7.2 会话排名 ····· 2-41
2.7.3 会话监控 ····· 2-42
3 安全分析 ····· 3-45
3.1 安全分析简介 ····· 3-45
3.2 安全事件分析 ····· 3-45
3.3 资产安全分析 ····· 3-47
3.4 WEB 防护分析 ····· 3-50

1 系统监控

系统监控是对系统当前状态信息的监控，主要包括在线用户、接口状态、黑名单记录、SSL VPN在线用户、实时流速监控和资产管理。

- 接口状态可以显示接口的状态、收发包速率、收发包总数等信息。
- 在线用户管理是对当前在线用户进行监控以及管理。包括对用户名、用户组IP地址、认证方式、在线时间、在线状态、登录时间等的详细记录，还可以对用户进行账户冻结。
- 黑名单记录可以通过IP和生命周期新建黑名单信息，还可以查看生成的黑名单记录，包括源IP、生命周期、生效时间、添加方式及状态信息。
- SSL VPN在线用户对当前SSL VPN在线用户进行监控以及管理。显示SSL VPN客户端接入的用户状态，可针对某一用户或某些用户进行冻结和强制注销。
- 实时流速监控可以显示用户实时流速、应用实时流速等信息。
- 资产管理提供以资产为核心的安全监控和分析理念，通过资产梳理、主动风险发现、被动流量检测，帮助用户构建对IT资产实现多维度的安全分析监控。
- 故障监控中心：对单用户终端网络状况进行监测。

1.1 在线用户管理

在导航栏中选择“数据中心>系统监控>在线用户”进入在线用户界面，如图 1-1 所示。

图1-1 在线用户管理

对在线用户管理详细说明如表 1-1 所示。

表1-1 在线用户管理说明

标题项	说明
用户名	通过设备上网的用户名称。
所属组	通过设备上网的用户所属的组。
IP地址	此用户所对应的IP地址。
认证方式	用户的认证方式。

标题项	说明
终端类型	用户的终端类型。
登录时间/冻结时间	用户第一次登录的时间或冻结时间。
状态	在线状态是正常还是被冻结，被冻结会显示冻结剩余时间，缺省是600秒。
在线时长	用户在线累计时间。
状态	用户的状态。
操作	冻结用户操作。

点击左侧用户组树的“根目录”，可以显示所有用户。

点击左侧用户组树的“属性组>匿名用户”，可以显示所有匿名用户。

点击左侧用户组树的“属性组>认证用户”，可以显示所有认证用户。

点击左侧用户组树的“属性组>移动用户”，可以显示所有移动用户。

点击用户右侧<锁定>按钮，可以锁定指定用户。

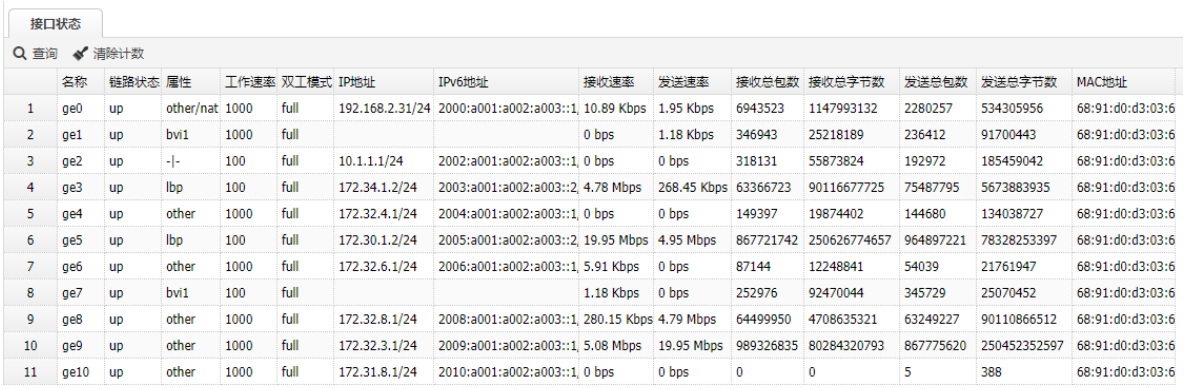
可以针对用户名和 MAC 地址进行模糊查询，输入查询条件后点击<查询>按钮进行查询。如图 1-2 所示。

图1-2 用户过滤条件

1.2 接口状态

在导航栏中选择“数据中心>系统监控>接口状态”进入接口状态显示界面，如图 1-3 所示。

图1-3 接口状态



	名称	链路状态	属性	工作速率	双工模式	IP地址	IPv6地址	接收速率	发送速率	接收总包数	接收总字节数	发送总包数	发送总字节数	MAC地址
1	ge0	up	other/nat	1000	full	192.168.2.31/24	2000:a001:a002:a003::1	10.89 Kbps	1.95 Kbps	6943523	1147993132	2280257	534305956	68:91:d0:d3:03:6
2	ge1	up	bvi1	1000	full			0 bps	1.18 Kbps	346943	25218189	236412	91700443	68:91:d0:d3:03:6
3	ge2	up	-|-	100	full	10.1.1.1/24	2002:a001:a002:a003::1	0 bps	0 bps	318131	55873824	192972	185459042	68:91:d0:d3:03:6
4	ge3	up	lbp	100	full	172.34.1.2/24	2003:a001:a002:a003::2	4.78 Mbps	268.45 Kbps	63366723	90116677725	75487795	5673883935	68:91:d0:d3:03:6
5	ge4	up	other	1000	full	172.32.4.1/24	2004:a001:a002:a003::1	0 bps	0 bps	149397	19874402	144680	134038727	68:91:d0:d3:03:6
6	ge5	up	lbp	100	full	172.30.1.2/24	2005:a001:a002:a003::2	19.95 Mbps	4.95 Mbps	867721742	250626774657	964897221	78328253397	68:91:d0:d3:03:6
7	ge6	up	other	1000	full	172.32.6.1/24	2006:a001:a002:a003::1	5.91 Kbps	0 bps	87144	12248841	54039	21761947	68:91:d0:d3:03:6
8	ge7	up	bvi1	100	full			1.18 Kbps	0 bps	252976	92470044	345729	25070452	68:91:d0:d3:03:6
9	ge8	up	other	1000	full	172.32.8.1/24	2008:a001:a002:a003::1	280.15 Kbps	4.79 Mbps	64499950	4708635321	63249227	90110866512	68:91:d0:d3:03:6
10	ge9	up	other	1000	full	172.32.3.1/24	2009:a001:a002:a003::1	5.08 Mbps	19.95 Mbps	989326835	80284320793	867775620	250452352597	68:91:d0:d3:03:6
11	ge10	up	other	1000	full	172.31.8.1/24	2010:a001:a002:a003::1	0 bps	0 bps	0	0	5	388	68:91:d0:d3:03:6

对接口状态的详细说明如表 1-2 所示。

表1-2 接口状态参数说明

标题项	说明
名称	接口名称
链路状态	接口的链路状态
属性	接口属性
工作速率	接口的工作速率
双工模式	接口的双工模式
IP地址	接口的IP地址
IPV6地址	接口的IPV6地址
接收速率	接口的接收报文速率
发送速率	接口的发送报文速率
接收总包数	接口接收报文总数
接收总字节数	接口接收报文总字节数
发送总包数	接口发送报文总数
发送总字节数	接口发送报文总字节数
MAC地址	接口MAC地址

点击左上角<清除计数>按钮可以立即清除当前的显示。

1.3 黑名单记录

1.3.1 黑名单概述

通过配置黑名单功能可以对来自指定 IP 地址的报文进行过滤，黑名单表项除了可以手工添加之外，还可以通过扫描攻击自动添加。

1.3.2 黑名单添加

通过菜单“数据中心 > 系统监控 > 黑名单记录”进入黑名单显示界面，如图 1-4 所示，点击<新建>按钮，将弹出添加黑名单界面，如图 1-5 所示。

图1-4 黑名单显示界面

图1-5 黑名单添加页面

表1-3 配置说明

配置项	说明
启用	勾选启用后黑名单生效，默认是勾选状态。
源IP	加入黑名单的IP地址，可以输入IPv4地址或IPv6地址，如：192.168.1.1或2000::1。
生命周期	对应IP地址加入黑名单的时长，可以单击下拉框选择，或者输入自定义秒数，输入范围1-2592000秒。

1.3.3 黑名单编辑

通过菜单“数据中心 > 系统监控 > 黑名单记录”进入黑名单显示界面，如图 1-6 所示，点击某条配置操作中的<编辑>按钮，将弹出编辑黑名单界面，如图 1-7 所示，可以对源 IP 和生命周期进行修改。黑名单配置各项参数含义如表 1-4 所示。

图1-6 黑名单显示界面

图1-7 黑名单编辑页面

表1-4 黑名单编辑配置说明

配置项	说明
启用	勾选启用后黑名单生效，默认是勾选状态。
源IP	加入黑名单的IP地址
生命周期	对应IP地址加入黑名单的时长

1.3.4 黑名单删除

通过菜单“数据中心 > 系统监控 > 黑名单记录”进入黑名单显示界面，如图 1-8 所示，点击某条配置操作中的<删除>按钮，或使用选择框选择黑名单配置，点击上方的<删除>按钮进行删除。

图1-8 黑名单显示界面

1.3.5 黑名单记录

黑名单可以配合某些防攻击模块一起使用，来达到更好的防护效果，比方说如果 IP 地址扫描攻击防护配置了加入黑名单，则当发生 IP 地址扫描攻击的时候，会自动生成一个源 IP 地址是攻击源地址的黑名单记录。

通过菜单“数据中心 > 系统监控 > 黑名单记录 > 黑名单记录”来查看所有添加的黑名单，如图 1-9 所示。

图1-9 黑名单记录显示界面

1.3.6 黑名单配置举例

1. 用户需求

将 IP 地址 3.3.3.3 加入黑名单，并设置周期为 10 分钟。

2. 配置步骤

(1) 如图 1-10 所示，通过菜单“数据中心 > 系统监控 > 黑名单记录”打开显示页面，点击<新建>按钮，在弹出的页面中进行配置，配置完成后点击<提交>按钮。

图1-10 黑名单添加页面

(2) 点击<提交>按钮后，完成黑名单的添加。

3. 验证配置

如图 1-11 所示，可以在显示页面看到刚刚添加的黑名单。

图1-11 黑名单显示页面

1.4 SSL VPN在线用户管理

在导航栏中选择“数据中心 > 系统监控 > SSL VPN 在线用户”，进入在线用户显示页面。页面中显示了已经拨入成功的 SSL VPN 用户。如图 1-12 所示。

图1-12 在线用户显示页面

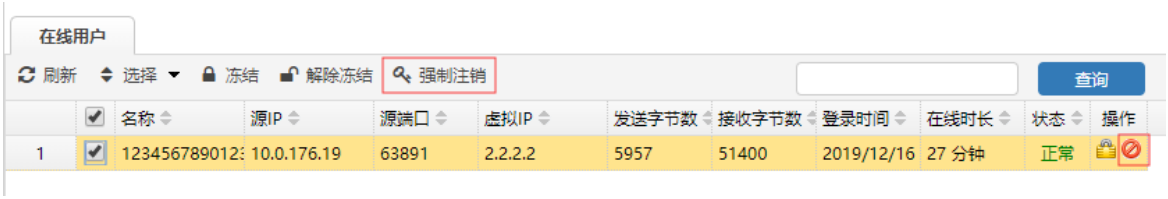
页面的详细说明如表 1-5。

表1-5 在线用户显示页面的详细说明

项目	说明
名称	SSL VPN拨入用户的名称。
源IP	SSL VPN拨入用户的源IP：一般是SSL VPN拨入用户公网出口IP地址
源端口	SSL VPN拨入用户的源端口。
虚拟IP	SSL VPN拨入用户分配到IP地址。
发送字节数	统计SSL VPN拨入用户发送字节数。
接收字节数	统计SSL VPN拨入用户接收字节数。
登录时间	SSL VPN用户登录成功时间。
在线时长	SSL VPN用户拨入后在线时长。
状态	SSL VPN拨入用户状态展示。
操作	可以对相应SSL VPN拨入用户进行的操作。

在线用户显示页面，点击<强制注销>按钮，可以将对应在线用户进行注销。如图 1-13 所示

图1-13 在线用户注销

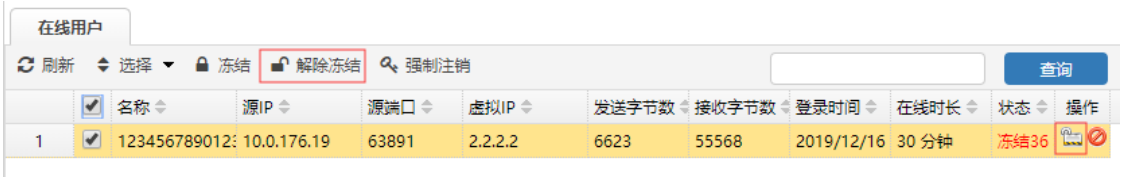


在线用户显示页面，点击<冻结>按钮，可以将对应的在线用户进行冻结。如图 1-14 所示

图1-14 在线用户冻结

在线用户显示页面，点击<解除冻结>按钮，可以将对应的已冻结用户解除冻结。如图 1-15 所示

图1-15 在线用户解除冻结

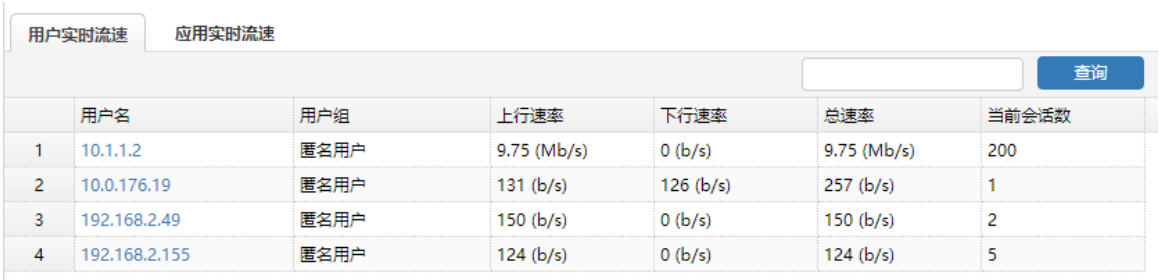


1.5 实时流速监控

1.5.1 用户实时流速

在导航栏中选择“数据中心 > 系统监控 > 实时流速监控”进入用户实时流速页面，如图 1-16 所示。

图1-16 用户实时流速



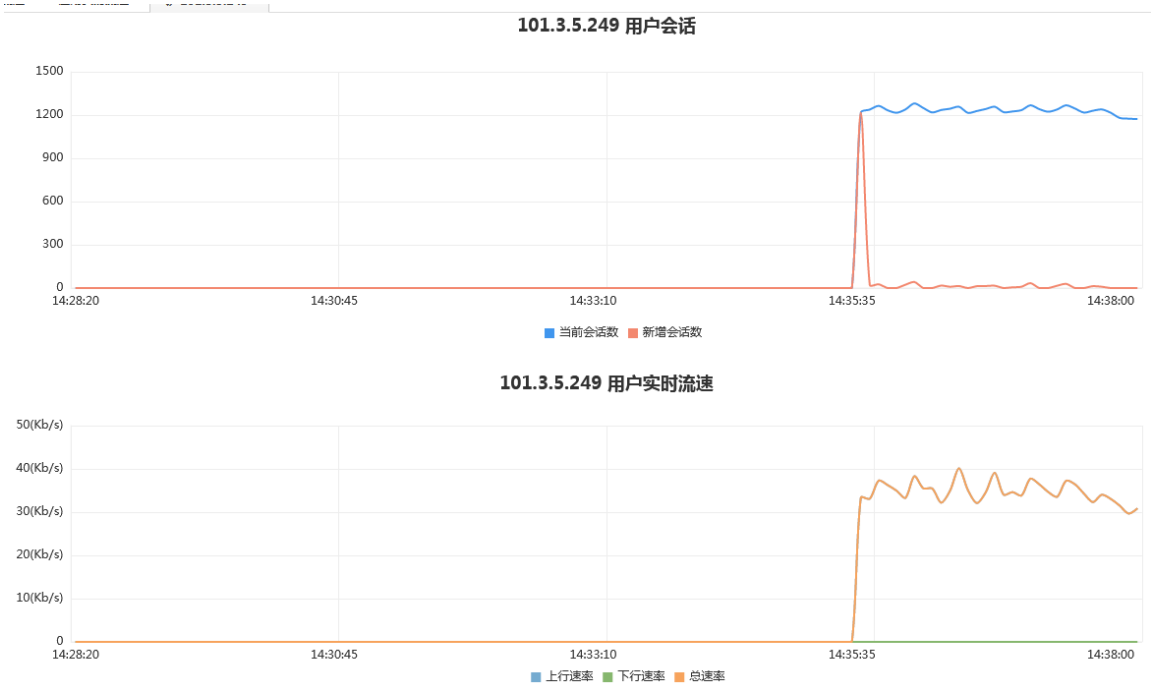
对设备用户实时流速的详细说明如表 1-6 所示。

表1-6 用户实时流速说明

标题项	说明
用户名	通过设备上网的用户名称
所属组	通过设备上网的用户所属的组
上行速率	显示该用户当前上行流速大小
下行速率	显示该用户当前下行流速大小
总流速	显示该用户当前上下行总流速大小
当前会话数	显示该用户当前会话数

点击“用户实时流速”里面的用户名列里面的用户名称，进入对应用户流量详细信息页面，如图 1-17 所示。

图1-17 对应用户流量详细信息页面



1.5.2 应用实时流速

在导航栏中选择“数据中心 > 系统监控 > 实时流速监控 > 应用实时流速”进入应用实时流速页面，如图 1-18 所示。

图1-18 应用实时流速

	应用名	上行速率	下行速率	总速率	当前会话数
1	其他TCP	25.37 (Mb/s)	1.98 (Mb/s)	27.34 (Mb/s)	1189
2	FTP文件传输协议	417.78 (Kb/s)	8.85 (Mb/s)	9.27 (Mb/s)	5
3	安全传输层协议(TLS)	2.47 (Mb/s)	178.02 (Kb/s)	2.65 (Mb/s)	363
4	Windows系统更新_下载	2.51 (Mb/s)	94.13 (Kb/s)	2.61 (Mb/s)	48
5	126邮箱_网页浏览	1.20 (Mb/s)	70.58 (Kb/s)	1.28 (Mb/s)	2
6	HTTP文件下载	973.71 (Kb/s)	41.38 (Kb/s)	1.02 (Mb/s)	5
7	SYSLOG日志	368.45 (Kb/s)	2.38 (Kb/s)	370.83 (Kb/s)	11
8	微软官网_网页浏览	286.99 (Kb/s)	19.26 (Kb/s)	306.25 (Kb/s)	85

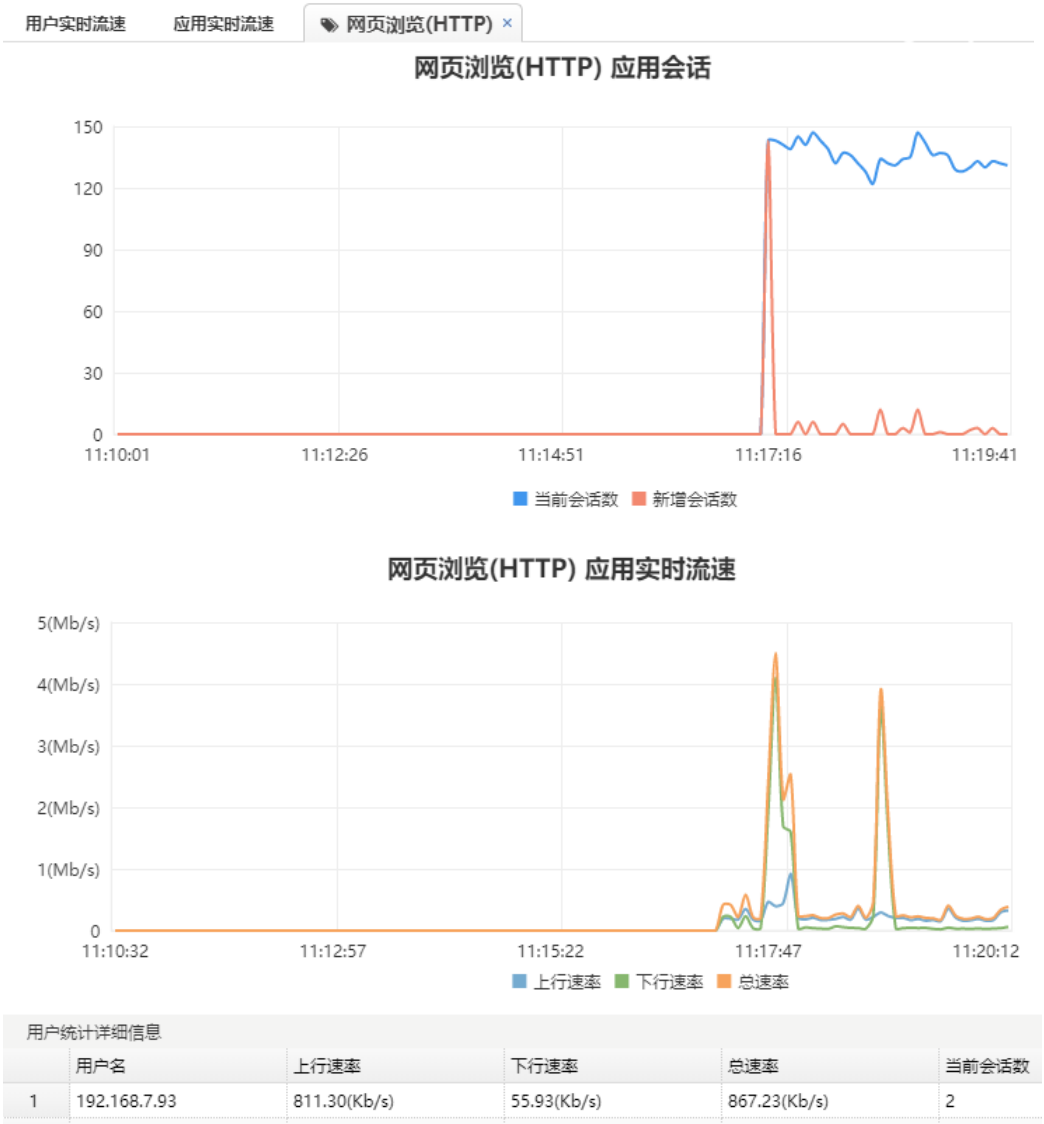
对设备应用实时流速的详细说明如表 1-7 所示。

表1-7 应用实时流速说明

标题项	说明
应用名	应用名称
上行速率	显示该应用当前上行流速大小
下行速率	显示该应用当前下行流速大小
总流速	显示该应用当前上下行总流速大小
当前会话数	显示该应用当前会话数

点击“应用实时流速”列表应用名列的应用名称，进入对应应用流量显示的详细页面，如图 1-19 所示。

图1-19 单个应用统计详细信息



对单个应用流量统计的详细说明如表 1-8 所示。

表1-8 单个应用流量统计说明

标题项	说明
用户名	用户名称
上行速率	应用的单个用户上行速率
下行速率	应用的单个用户下行速率
总流量	应用的单个用户上下行总速率
当前会话数	应用的单个用户当前会话数

1.6 资产管理

1.6.1 资产管理概述

提供以资产为核心的安全监控和分析理念，通过资产梳理、主动风险发现、被动流量检测，帮助用户构建对 IT 资产实现多维度的安全分析监控。

从扫描、检测、感知三个维度进行风险发现，帮助企业做到：事前预防、事中阻断、事后回溯，提供一套全新的资产风险感知的解决方案。

资产识别涉及以下概念：

- 资产识别设定：开启资产识别设定后，可以通过流量识别资产信息。
- 端口扫描：端口扫描时勾选资产同步功能，可以将端口扫描结果同步到资产信息中。
- 可以识别到 IPv4 以及 IPv6 地址的资产

资产管理的配置思路：

(1) 配置资产识别范围，决定需要对哪些地址范围进行流量识别，资产 IP 支持 IPv4/IPv6 地址。

(2) 配置端口扫描任务，并勾选资产识别同步功能，资产识别设定的 IP 支持 IPv4/IPv6 地址。

1.6.2 资产管理配置

通过菜单“数据中心 > 系统监控 > 资产管理”，进入资产管理页面，如图 1-20 所示界面。

图1-20 资产管理

表1-9 资产管理详细表项说明

参数	说明
新建	手动新建资产信息
导入	支持导入资产信息
导出	支持导出资产信息
查询	可以按照资产IP、资产描述、用户、部门、重要度、操作系统、可用服务、状态、服务标识组合查询
同步策略状态	同步资产IP所对应的控制策略ID
资产IP	资产IP地址，支持IPv4/IPv6地址。
资产描述	资产的描述信息

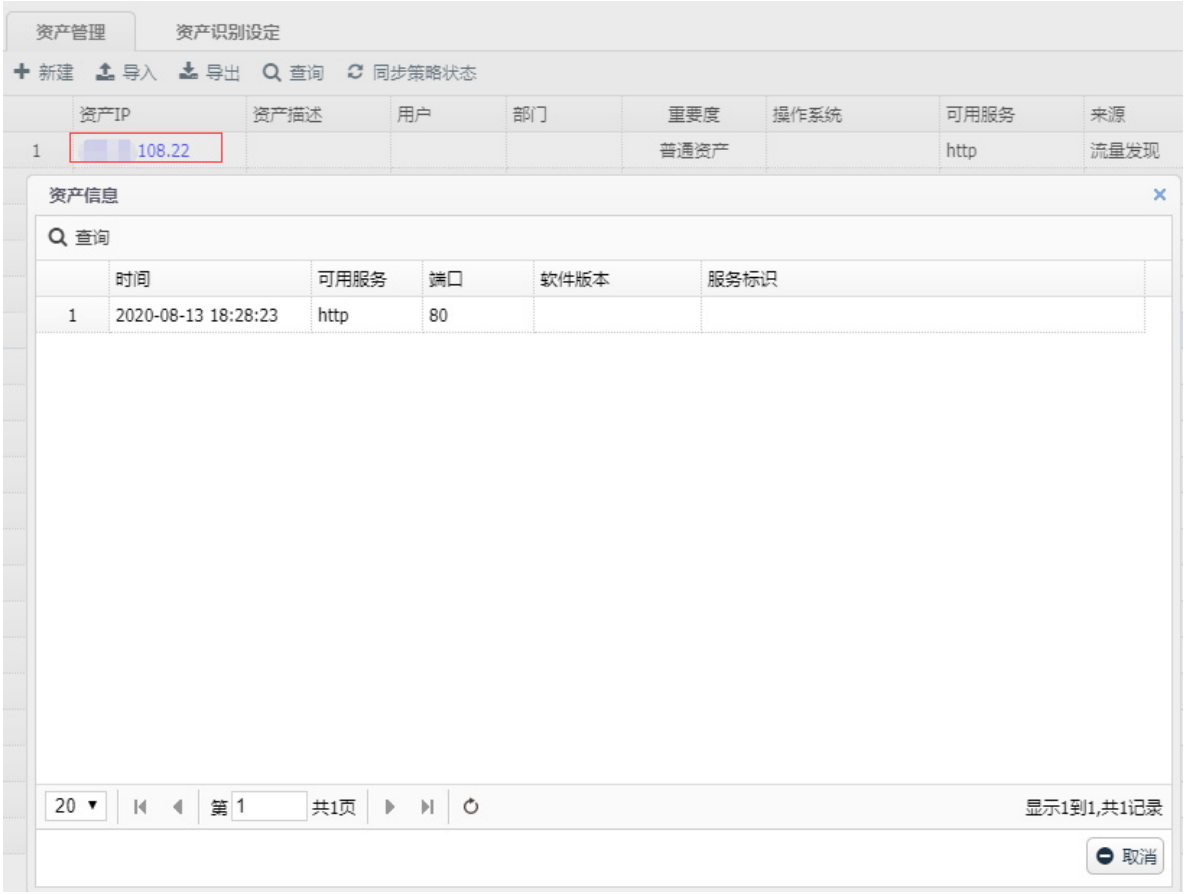
参数	说明
用户	资产所属用户
部门	资产所属用户的部门
重要度	资产的重要度
操作系统	资产使用的操作系统
可用服务	资产使用的服务
来源	资产的来源方式
状态	资产的状态 ● 活跃：设备在线 ● 空闲：设备离线
操作	支持编辑和删除资产

点击“同步策略状态”可以同步资产 IP 所对应的控制策略 ID。系统会根据资产的源 IP 和目的 IP，对控制策略进行匹配，将命中的策略 ID 同步到资产管理列表中。同步成功后，点击资产管理列表中对应的控制策略 ID，即可查看对应的控制策略信息。如下图所示。

图1-21 控制策略信息页面

如果识别出资产的可用服务后，在资产管理列表中点击对应的资产 IP，可以查看资产可用服务的详细信息，如下图所示。

图1-22 资产详细信息页面



1.6.3 资产识别设定

通过菜单“数据中心 > 系统监控 > 资产管理 > 资产识别设定”，进入资产识别设定页面，如图 1-23 所示。

图1-23 资产识别设定

表1-10 资产识别设定配置项含义描述表

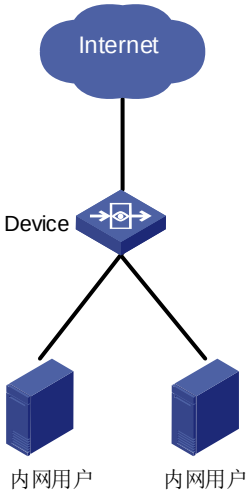
参数	说明
开启	开启资产识别功能
地址项目	支持资产按照子网地址、范围地址和主机地址等方式添加，可输入IPv4地址或IPv6地址，最多可配置50条。
排除地址	排除识别资产的地址
已添加服务标识	支持识别自定义服务标识

1.6.4 资产识别配置举例

1. 组网需求

内网用户通过设备访问 Internet，需要实时监控内网资产情况。

图1-24 资产识别案例拓扑图



2. 配置步骤

(1) 配置资产识别设定。

在导航栏中选择“数据中心 > 系统监控 > 资产管理 > 资产识别设定”进入资产识别设定页面，如图1-25 所示，配置完成后点击<提交>按钮。

图1-25 资产识别设定

(2) 配置端口扫描功能。

在导航栏中选择“策略配置 > 安全设置 > 风险扫描 > 端口扫描 > 端口扫描任务”，单击“新建”按钮，进入端口扫描任务配置页面，如图 1-26 所示，配置完成后点击<提交>按钮。

图1-26 端口扫描

3. 验证配置

在导航栏中选择“数据中心 > 系统监控 > 资产管理”，进入资产管理页面，可以查看到识别的资产信息，如图 1-27 所示。

图1-27 资产管理

	资产IP	资产描述	用户	部门	重要度	操作系统	可用服务	来源	状态	操作
1	192.168.199.168				普通资产		microsoft-ds	流量发现	空闲	编辑 删除
2	10.0.138.208		10.0.138.208	匿名用户组	普通资产			流量发现	空闲	编辑 删除
3	192.168.9.113		192.168.9.113	匿名用户组	普通资产			流量发现	空闲	编辑 删除
4	192.168.6.171		192.168.6.171	匿名用户组	普通资产			流量发现	空闲	编辑 删除
5	192.168.202.53		192.168.202.5	匿名用户组	普通资产	windows		流量发现	活跃	编辑 删除
6	192.168.9.130		192.168.9.130	匿名用户组	普通资产			流量发现	活跃	编辑 删除
7	10.0.250.19		10.0.250.19	匿名用户组	普通资产			流量发现	空闲	编辑 删除
8	192.168.203.2				普通资产			流量发现	活跃	编辑 删除
9	192.168.9.131		192.168.9.131	匿名用户组	普通资产			流量发现	空闲	编辑 删除

1.7 故障监控中心

1.7.1 简介

当设备管理员需要了解某个终端用户或 IP 的网络状况而又不便于操作这个终端时，可以使用单用户检测功能探测终端网络状况，便于网络维护和管理。主要检测内容包括通用及自定义地址 DNS 测试、并发连接测试、通用及自定义地址带宽测试、终端性能测试等。

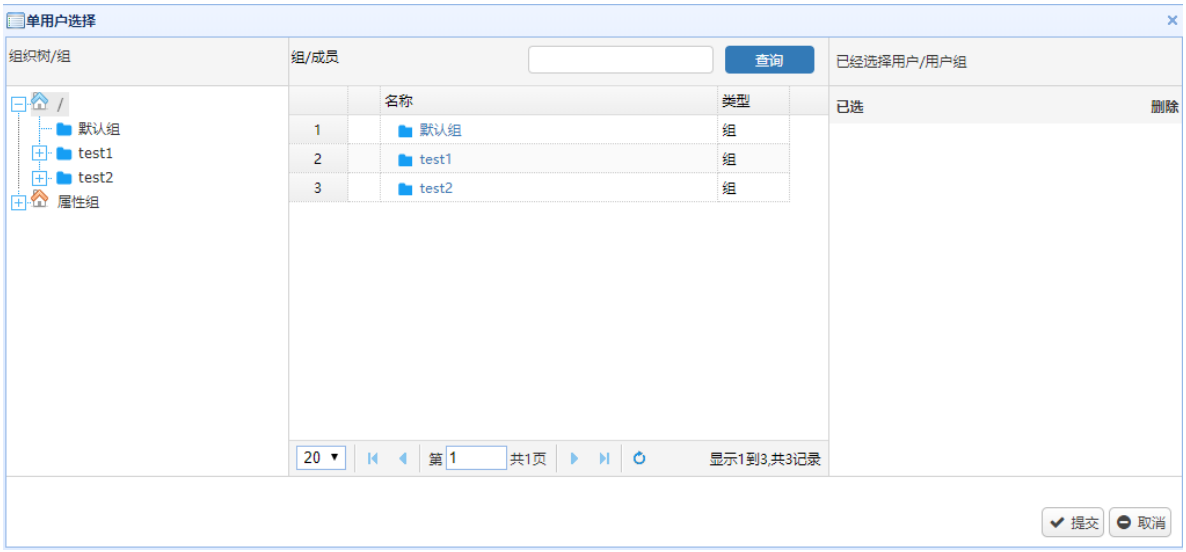
1.7.2 单用户检测配置

在导航栏中选择“数据中心 > 系统监控 > 故障监控中心 > 单用户检测”进入单用户检测页面，如下图所示。

图1-28 单用户检测页面

监测对象可以配置为 IP 地址（匿名用户使用）或者用户名，配置匿名用户时必须为在线用户；也可以单击“选择用户”从用户组或属性组中选择单个用户，如下图所示。

图1-29 单用户选择



在单用户检测页面，单击监测地址后面的“设置”，进入监测地址配置界面，如下图所示。

图1-30 监测地址配置界面

监测地址配置界面参数如表 1-11 所示。

表1-11 监测地址配置参数说明

参数	说明
终端页面重定向	重定向至测试页面的终端页面。可选择访问百度时（news.baidu.com）重定向至测试页面，也可以选择访问所有Web页面时重定向至测试页面。
监测地址	需要对终端用户进行网络监测的地址，作为DNS、并发连接、带宽测试使用。可以使用内置监测地址库，也可以自定义。 如果用户访问内置监测地址不通，可以配置自定义监测地址。 自定义监测地址格式支持域名、域名+端口、不带路径的URL（例：www.example.com、www.example.com:8080、http://www.example.com）一行支持一个域名，回车换行，最多支持8个。

说明

- 自定义监测地址不支持 https 网站。
- 如果多个终端使用同一个认证用户上网，终端都会推送测试页面，但只能监测一个终端。
- 若探测用户名为 IP 地址，则只针对此 IP 地址的用户进行单用户检测，不会检测此 IP 地址的匿名用户。
- 默认只支持 http 网站进行重定向，可以通过 user-policy https-portal enable 命令开启 https 网站重定向。

单击“开始监测”按钮，设备端会显示正在等待终端用户访问，如图 1-31 所示。

图1-31 开始监测界面

开始监测后，如果用户终端一直无请求，则 5 分钟后设备端页面会提示用户测试超时；单击“取消监测”可以停止监测。

如果用户终端开启测试，测试完成后设备端页面会显示最终测试结果，若测试质量差，会显示网络诊断信息。

1.7.3 单用户检测配置举例

1. 组网需求

使用自定义监测地址对内网终端用户进行网络检测，终端用户访问百度（news.baidu.com）重定向至测试页面。

2. 配置前提

(1) 完成基础网络配置。设备需要通过路由模式或者网桥模式部署，如果是网桥模式，必须要在网桥接口上配置 IP 地址。

(2) 内部网络用户通过设备可以上网。

3. 配置步骤

(1) 在设备侧配置单用户检测

通过菜单“数据中心 > 系统监控 >故障监控中心 > 单用户检测”，进入单用户检测页面，配置监测对象，并输入自定义监测地址，单击“开始监测”。

图1-32 单用户检测配置页面

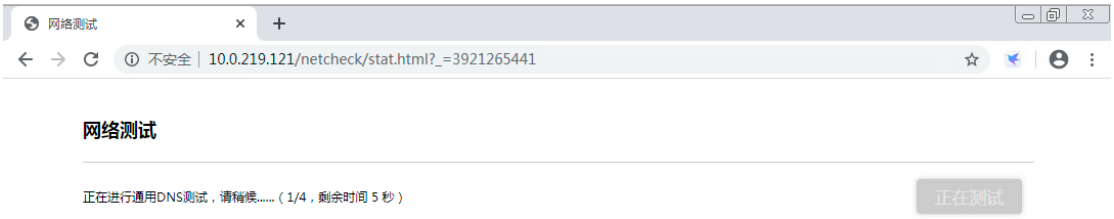
(2) 用户侧重定向到测试页面

测试用户打开浏览器并访问 news.baidu.com，会重定向到测试页面，如下图所示。

图1-33 用户侧重定向页面

测试用户单击“开始测试”，此时测试用户与设备开始进行交互。用户侧页面如下图所示。

图1-34 用户侧开始测试页面



(3) 设备侧开始监测

测试用户单击“开始测试”后，设备侧显示监测信息，如下图所示。

4. 验证配置

测试完成后，用户侧显示测试完成的提示信息，如图 1-35 所示。设备侧会显示最终测试结果，如果测试质量差，会显示诊断信息，如图 1-36 所示。

图1-35 用户侧测试完成页面

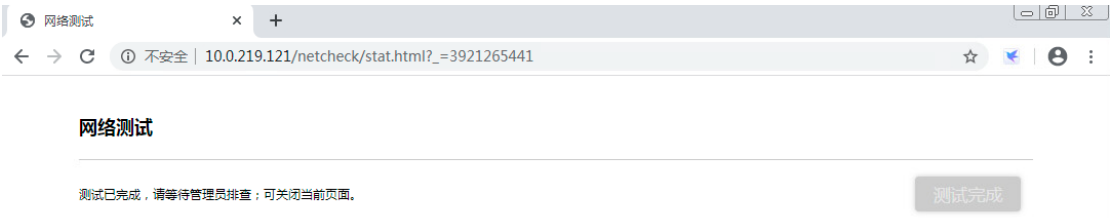


图1-36 设备侧测试完成页面

2 数据分析

2.1 数据分析简介

数据分析是对系统应用及设备流量等产生的数据进行统计分析，包括用户流量统计、应用流量统计、用户信息中心、设备流量统计、设备健康统计和会话监控统计。

- 用户流量统计以柱状图、表格形式展示用户流量信息。
- 应用流量统计以趋势图、饼状图、表格形式展示应用流量信息。
- 用户信息中心包含用户日志统计、用户访问网站分析、用户轨迹时光轴等信息。
- 设备流量统计可以显示指定条件下设备流量信息。
- 设备健康统计可以显示整机转发流量、会话数、cpu、内存使用等信息。
- 会话监控统计可以显示设备会话统计、会话排名、会话监控等信息。

2.2 用户流量统计

在导航栏中选择“数据中心 > 数据分析 > 用户流量统计”进入用户流量统计页面，如图 2-1 所示。

图2-1 用户流量统计

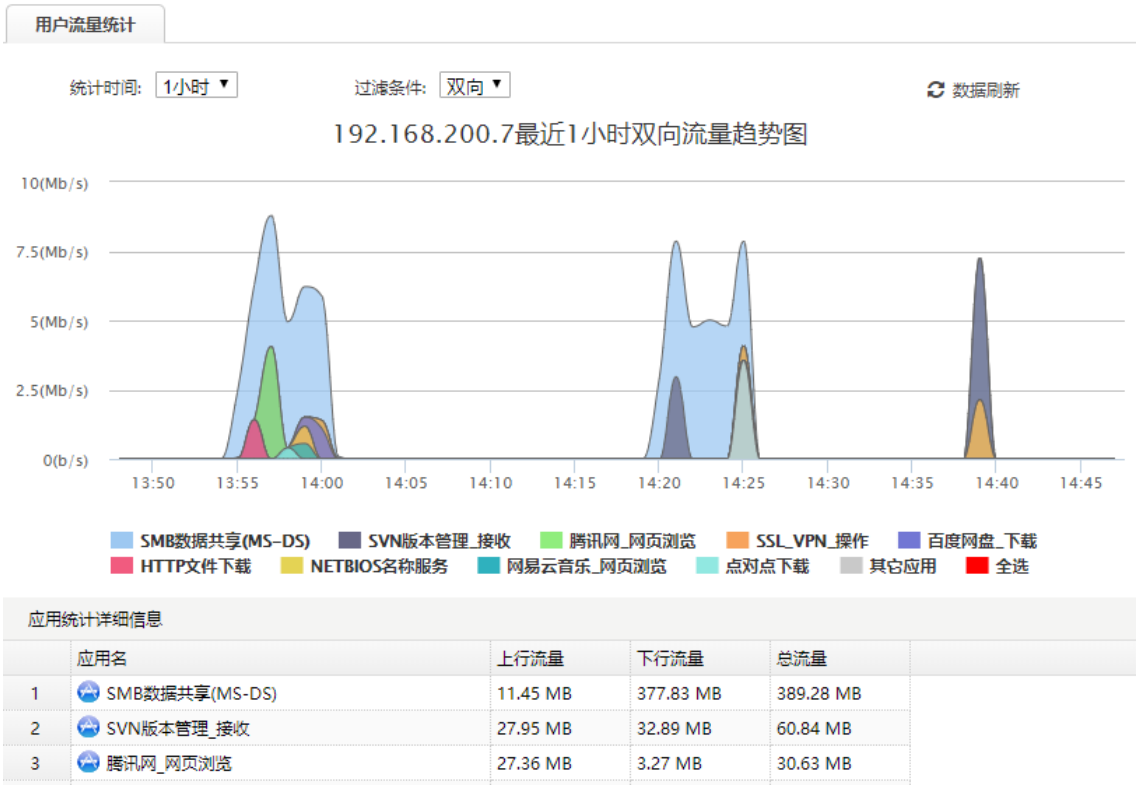
对用户流量统计的详细说明如表 2-1 所示。

表2-1 用户流量说明

标题项	说明
统计时间	设定流量显示的时间跨度，可选的值有： • 最近一小时 • 最近一天 • 最近一周 缺省情况下，显示最近一小时的用户流量统计
过滤条件	过滤显示流量的方向，可选的值有： • 双向 • 上行 • 下行 缺省情况下，显示双向的用户流量统计
刷新数据	立即刷新显示的统计数据
用户名	用户的名称
上行流量	用户的上行流量
下行流量	用户的下行流量
总流量	用户的上下行流量总和

点击“用户统计详细信息”表格里面的用户名列里面的用户名称，进入对应用户详细流量统计的页面，如图 2-2 所示。

图2-2 单个用户流量统计信息



应用统计详细信息

	应用名	上行流量	下行流量	总流量
1	SMB数据共享(MS-DS)	11.45 MB	377.83 MB	389.28 MB
2	SVN版本管理_接收	27.95 MB	32.89 MB	60.84 MB
3	腾讯网_网页浏览	27.36 MB	3.27 MB	30.63 MB

单个用户的流量统计的详细说明如表 2-2 所示。

表2-2 单个用户流量统计说明

标题项	说明
应用名	应用的名称
上行流量	用户的单个应用的上行流量
下行流量	用户的单个应用的下行流量
总流量	用户的单个应用的上下行总流量

2.3 应用流量统计

在导航栏中选择“数据中心 > 数据分析 > 应用流量统计”进入应用流量统计显示页面，如图 2-3 所示。向下拖动下拉按钮，显示最近一段时间的总流量占比图，如图 2-4 所示。页面最下方是应用统计详细信息，如图 2-5 所示。

图2-3 应用流量统计趋势

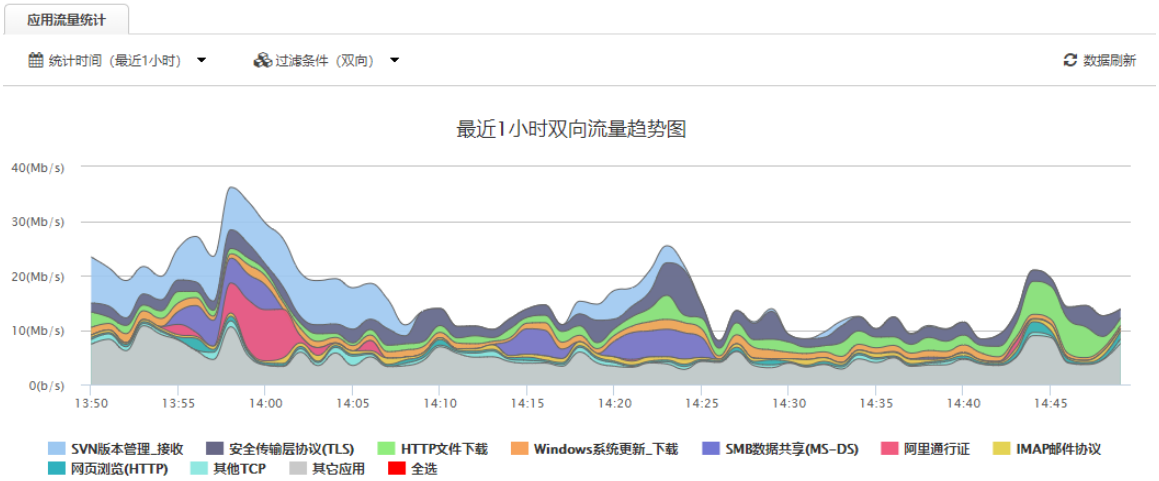


图2-4 应用流量占比

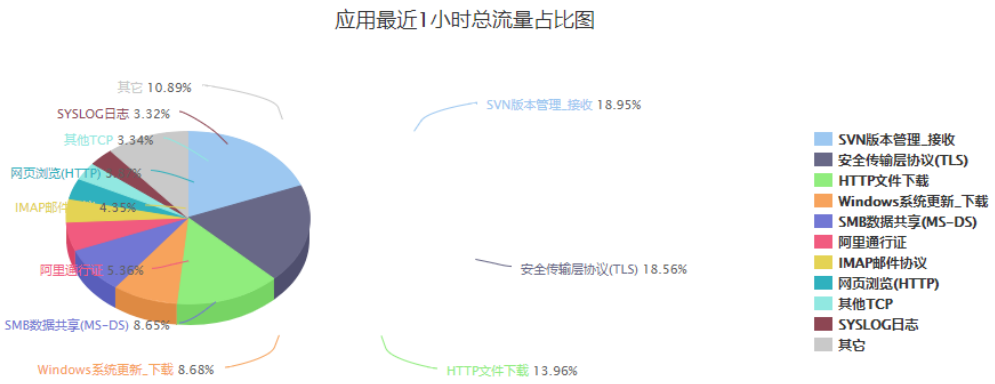


图2-5 应用统计显示详细信息

应用统计详细信息

	应用名	上行流量	下行流量	总流量
1	网页浏览(HTTP)	76.51 KB	65.27 KB	141.78 KB
2	UDP	132.90 KB	170 B	133.07 KB
3	QQ	9.41 KB	53.59 KB	63.01 KB
4	网页图片浏览/下载	10.89 KB	41.78 KB	52.67 KB
5	NETBIOS名称服务	39.38 KB	1.95 KB	41.33 KB
6	TCP	24.99 KB	8.68 KB	33.67 KB
7	简单服务发现协议(SSDP)	25.70 KB	0 B	25.70 KB
8	多播名称解析(mDNS)	23.23 KB	0 B	23.23 KB
9	安全传输层协议(TLS)	7.10 KB	15.95 KB	23.05 KB
10	域名解析协议(DNS)	4.10 KB	11.85 KB	15.94 KB

对应用流量统计的详细说明如表 2-3 所示。

表2-3 应用流量统计说明

标题项	说明
统计时间	设定流量显示的时间跨度，可选的值有： • 最近一小时 • 最近一天 • 最近一周 缺省情况下，显示最近一小时的应用流量统计
过滤条件	过滤显示流量的方向，可选的值有： • 双向 • 上行 • 下行 缺省情况下，显示双向的应用流量统计
刷新数据	立即刷新应用流量统计信息

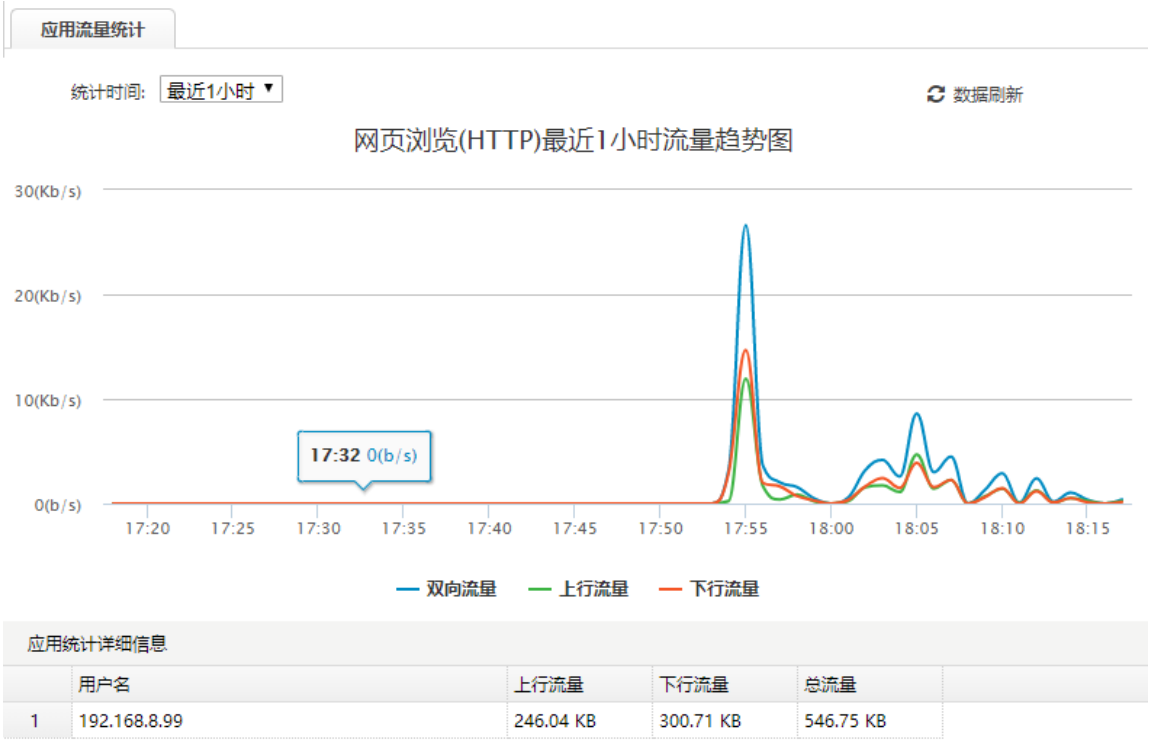
对应用统计详细信息的说明如表 2-4 所示。

表2-4 应用统计详细信息说明

标题项	说明
应用名	应用的名称
上行流量	应用的上行流量
下行流量	应用的下行流量
总流量	应用的总流量

点击“应用统计详细信息”表格里面应用名列的应用名称，进入对应应用流量显示的详细页面，如图 2-6 所示。

图2-6 单个应用统计详细信息



对单个应用流量统计的详细说明如表 2-5 所示。

表2-5 单个应用流量统计说明

标题项	说明
用户名	用户名称
上行流量	用户的单个应用上行流量
下行流量	用户的单个应用下行流量
总流量	用户的单个用上下行总流量

2.4 用户信息中心

在导航栏中选择“数据中心 > 数据分析 > 用户信息中心”进入用户信息中心显示界面，如图 2-7 所示。

图2-7 用户信息中心

	用户名	用户组	IM聊天	社区	搜索引擎	文件传输	邮件	网络娱乐	其它	网站访问
1		测试	3036	1	14	2	36	0	18	333
2		测试	59	0	0	1797	18	0	191	831
3		测试	61	0	0	645	84	0	75	5092
4	192.168.4.89	匿名用户组	50	0	2	11	3	0	0	659
5		产品	33	0	0	26	50	0	0	630
6	192.168.4.86	匿名用户组	179	0	0	2	13	0	0	65
7	192.168.1.119	匿名用户组	51	0	0	4	0	0	3	166

对用户信息中心的详细说明如表 2-6 所示。

表2-6 用户信息中心说明

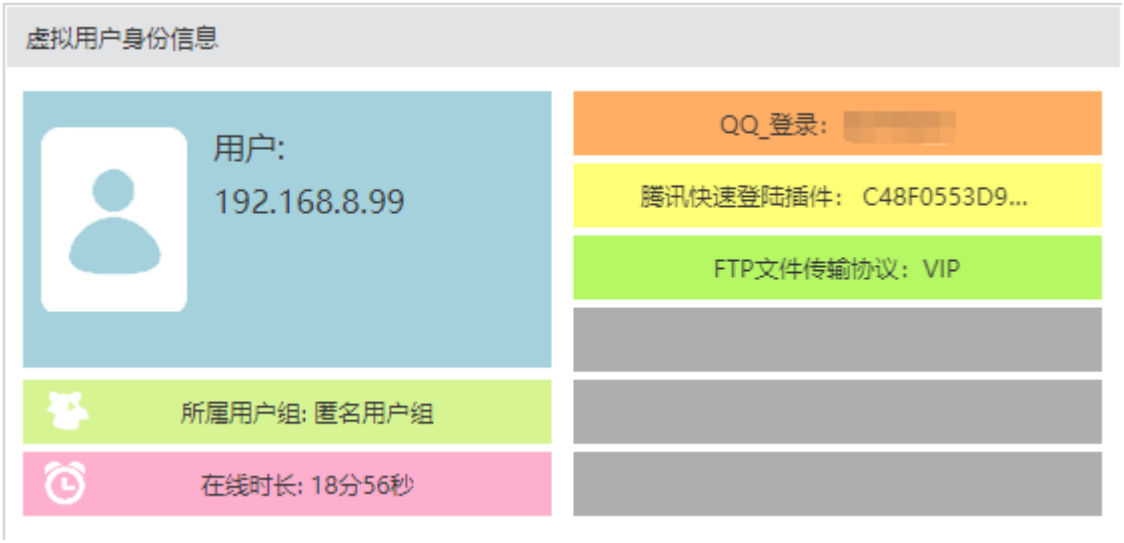
标题项	说明
选择日期	缺省情况，显示当天用户的基本日志量的信息。
用户过滤	输入用户名关键字，展现经过滤的用户信息列表。
用户名	用户名称
用户组	用户所属用户组
IM聊天	IM聊天日志的条数目
社区	社区日志的条目数
搜索引擎	搜索引擎日志的条目数
文件传输	文件传输日志的条目数
邮件	邮件收发记录日志的条目数
网络娱乐	网络娱乐应用日志的条目数
其它	其它应用的日志条目数
网站访问	访问网站记录的日志条目数

在用户中心的用户基础信息列表，选择某个用户进入该用户的用户数据中心页面。

2.4.1 虚拟用户身份

用户中心的虚拟用户身份信息如图 2-8 所示。

图2-8 虚拟用户身份



对虚拟用户身份信息的详细说明表 2-7 所示。

表2-7 虚拟用户身份信息说明

标题项	说明
用户	用户名称
所属组	用户所属的组
在线时长	用户在线累计时间

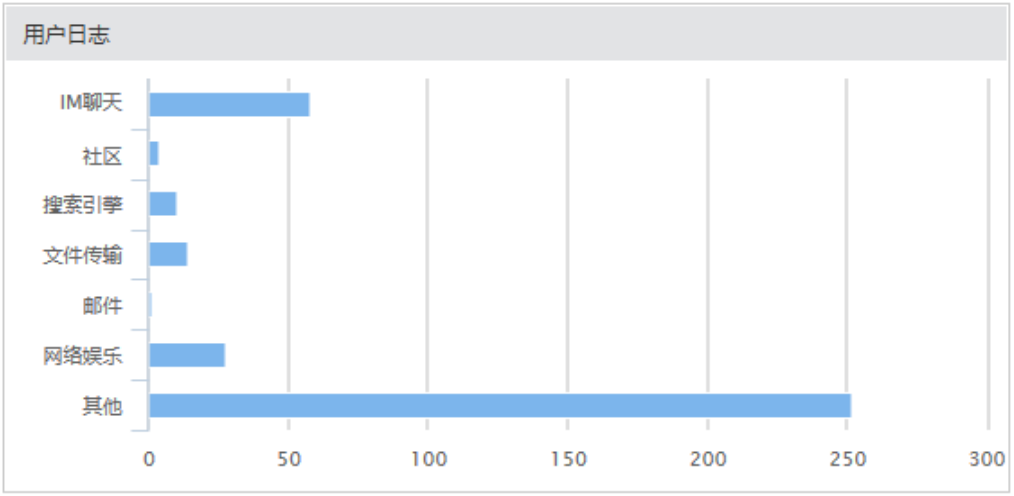
说明

虚拟用户身份信息中显示用户登录的虚拟身份账号信息，其中微信的身份信息，是微信用户的 uin，即 user information，是微信用户信息的身份标识。uin 是微信用户的唯一识别码，不是用户登录微信的账号。

2.4.2 用户日志统计

用户中心的用户日志数统计图 2-9 所示。

图2-9 用户日志统计



对用户日志数量统计图的详细说明如表 2-8 所示。

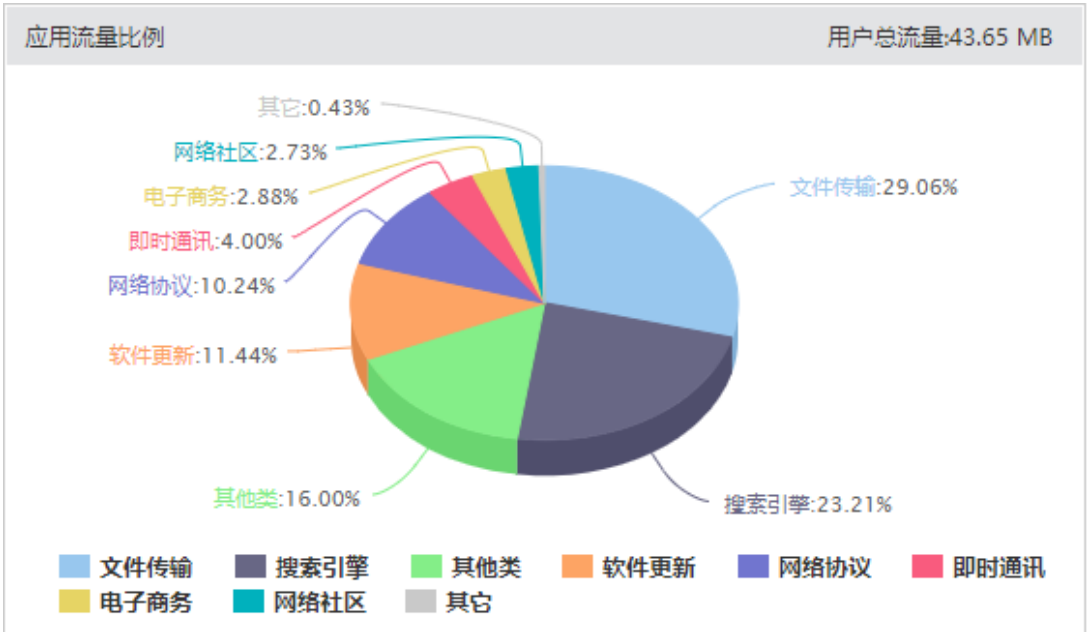
表2-8 用户日志统计说明

标题项	说明
IM聊天	当天该用户产生的IM聊天日志条数
社区	当天该用户产生的社区日志条数
搜索引擎	当天该用户产生的搜索引擎日志条数
文件传输	当天该用户产生的文件传输日志条数
邮件	当天该用户产生的邮件日志条数
网络娱乐	当天该用户产生的网络娱乐日志条数
其它	当天该用户产生的其它日志条数

2.4.3 应用流量比例

用户中心的应用流量比例如图 2-10 所示。

图2-10 应用流量比例

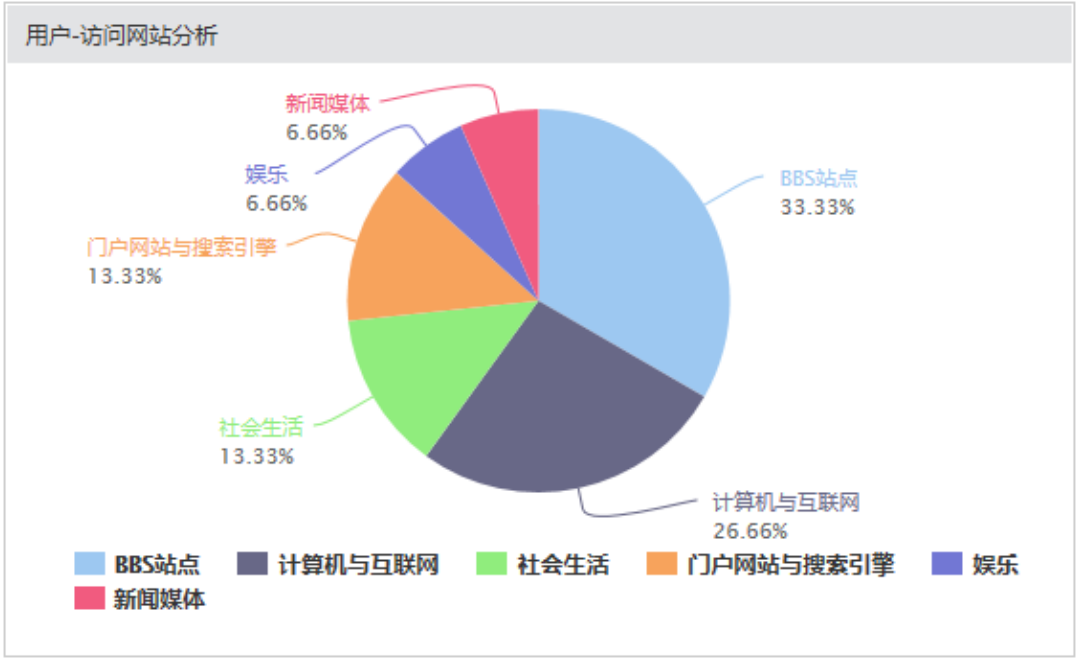


对应用流量比例统计的说明，表框右上角显示该用户当天的总流量，饼图展示该用户当天应用类流量的占比。

2.4.4 用户-访问网站分析

用户中心的用户-访问网站分析如图 2-11 所示

图2-11 用户-访问网站分析



用户-访问网站分析的饼图主要展示该用户当天访问不同类型网站的比例。

2.4.5 用户轨迹时光轴

用户中心的用户轨迹时光轴展示如图 2-12 所示

图2-12 用户轨迹时光轴

用户轨迹时光轴主要展现该用户当天的主要网络行为事件。时光轴左侧表示用户核心事件触发的时间点，右侧展示用户核心事件的具体内容。

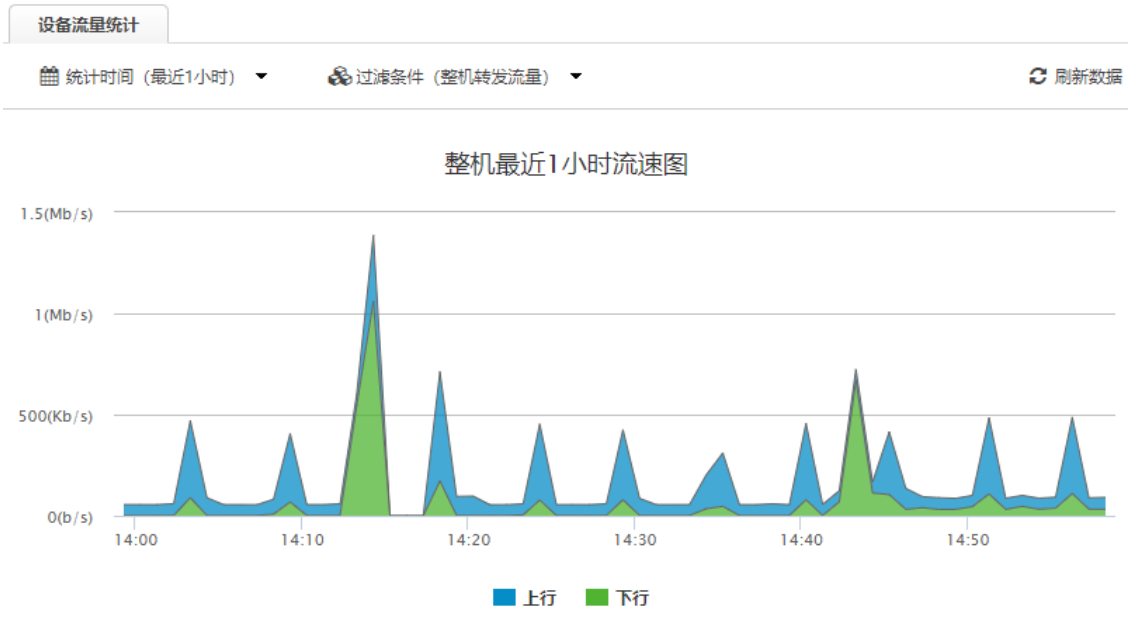
说明

如果用户时光轴信息中有微信登录的事件信息时，此处展示的登录微信的账号为微信用户的 uin，即 user information，是微信用户信息的身份标识。uin 是微信用户的唯一识别码，不是用户登录微信的账号。

2.5 设备流量统计

在导航栏中选择“数据中心 > 数据分析 > 设备流量统计”进入设备流量统计页面，如图 2-13 所示。

图2-13 设备流量统计详细信息



对设备流量统计的详细说明如表 2-9 所示。

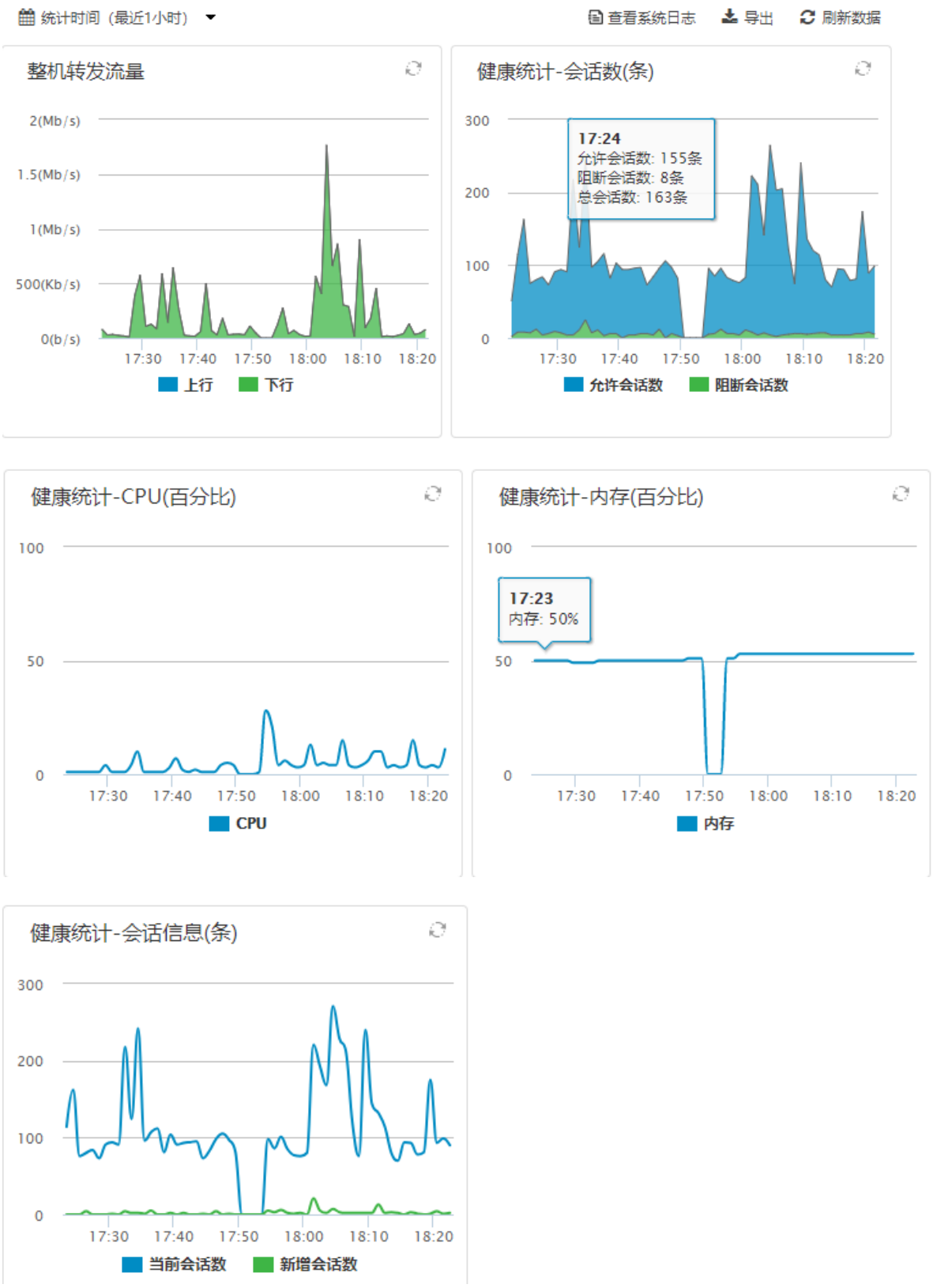
表2-9 设备流量统计说明

标题项	说明
统计时间	设定流量显示的时间跨度，可选的值有： • 最近一小时 • 最近一天 • 最近一周 缺省情况下，显示最近一小时的用户流量统计
过滤条件	过滤显示流量的接口，可选值有： • 整机转发流量 • 特定某个接口的流量 缺省情况下，显示整机转发流量的统计
刷新数据	立即刷新显示的统计数据
上行、下行	不同显色显示设备的上下行流量，点击可以在现实上显示/取消显示该项流量 缺省情况下，上下行流量都显示

2.6 设备健康统计

在导航栏中选择“数据中心 > 数据分析 > 设备健康统计”进入设备健康统计页面，如图 2-14 所示。

图2-14 设备健康统计详细信息



对设备健康统计的详细说明如表 2-10 所示。

表2-10 设备健康统计说明

标题项	说明
统计时间	设定健康统计显示的时间维度，可选的值有： • 最近 1 小时 • 最近 4 小时 • 最近 1 天 • 最近 1 周 缺省情况下，显示最近1小时的设备健康统计数据。
刷新数据	立即刷新显示的所有健康统计项的统计数据
每幅图的刷新图标	立即刷新健康统计当前项的显示的统计数据
整机转发流量	设备整机的吞吐量曲线图，点击图下的上下行图标，可以选择： 上行：设备外网口的发包流量统计。 下行：设备内网口的发包流量统计。 缺省状态下，显示上行和下行。
健康统计-会话数	设备的会话数统计，点击图下的允许会话数和阻断会话数图标可以选择： 允许会话数：设备允许创建的会话数。 阻断会话数：设备因各种原因被阻断的会话。 缺省情况下，显示允许和阻断会话数。
健康统计-CPU（百分比）	显示设备的CPU使用率，以百分比显示。
健康统计-MEM（百分比）	显示设备的内存使用情况，以百分比显示。
健康统计-会话信息	设备的会话信息统计，点击图下的当前会话数和新增会话数图标可以选择： 当前会话数：设备当前已创建的会话数。 新增会话数：设备当前新增的会话。 缺省情况下，显示当前会话数、当前新增会话数和当前总会话数。

点击“导出”按钮，可以导出设备一周内的详细健康统计信息，导出设置页面如 2-15 设备健康统计信息导出页面所示，导出的数据表格如图 2-16 所示。

图2-15 设备健康统计信息导出页面

图2-16 导出的数据表格

对导出页面阈值的设置详细说明如表 2-11 所示。

表2-11 阈值设置说明

标题项	说明
整机流量	默认勾选，阈值为0，即全部导出，最大值为10G。
会话允许/阻断	默认勾选，阈值为0，即全部导出，最大值为30w条。
CPU百分比	默认勾选，阈值为0，即全部导出，最大值为100%。

标题项	说明
内存百分比	默认勾选，阈值为0，即全部导出，最大值为100%。
会话数	默认勾选，阈值为0，即全部导出，最大值为30w条。

2.7 会话监控统计

2.7.1 会话统计

通过菜单“数据中心 > 数据分析 > 会话监控统计 > 会话统计”，进入如图 2-17 所示页面。在该页面可以查看会话相关统计信息。

图2-17 会话统计页面

会话统计详细说明如表 2-12 所示。

表2-12 会话统计详细说明表

标题项	说明
会话数	统计设备当前的总会话数以及新增会话数，通过曲线进行展示。
历史会话统计	统计设备上最近一段时间（最近1小时、最近1天、最近1周）的历史会话数，以TCP、UDP、其它维度进行统计，通过趋势图进行展示。
会话源目标排名	基于源地址排名的TOP20会话数排名。
会话目的目标排名	基于目的地址排名的TOP20会话数排名。

2.7.2 会话排名

通过菜单“数据中心 > 数据分析 > 会话监控统计 > 会话排名”，进入如图 2-18 所示页面。在该页面可以基于条件查看基于源地址、目的地址、目的端口排名的会话。

图2-18 会话排名页面

点击页面上的<查询>按钮，可以基于会话统计过滤条件查询会话排名。查询页面如图 2-19 所示。

图2-19 会话排名查询页面

会话排名详细说明如表 2-13 所示。

表2-13 会话排名详细说明表

标题项	说明
统计类型	统计类型主要有源地址、目的地址、目的端口三个维度进行统计，默认是源地址维度统计。
统计值	基于统计类型查询TOP N的会话排名上的具体会话IP地址。
连接数	会话上对应的连接个数。
会话过滤	点击会话过滤可以直接查看该会话的详细会话列表，直接跳转到会话监控页面展示。

2.7.3 会话监控

通过菜单“数据中心 > 数据分析 > 会话监控统计 > 会话监控”，进入如图 2-20 所示页面。在该页面可以查看设备上的详细会话，也可以根据指定条件查询会话信息。

图2-20 会话监控页面

会话监控页面默认会话列展示项详细说明如表 2-14 所示。

表2-14 会话监控页面默认会话列展示项详细说明表

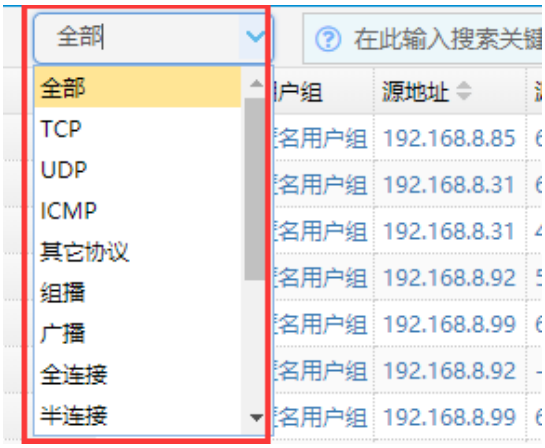
标题项	说明
用户	用户组织结构上对应的用户名，如用户不在识别范围内，此项显示为空。
用户组	用户组织结构上对应的用户组，如用户不在识别范围内，此项显示为空。
源地址	会话发起方IP地址或根据识别范围配置确定的源IP地址。
源端口	与源地址同一方的端口。
目的地址	会话响应方IP地址或根据识别范围配置确定的目的IP地址。
目的端口	与目的地址同一方的端口。
协议	IP协议号，TCP/UDP/ICMP/IGMP，如果有其它的协议，直接显示协议号。
类型	会话连接类型，主要有半连接和全连接两种。
应用	应用识别模块审计到会话访问的应用。
发送流量	会话发送的字节。
接收流量	会话接收的字节。
总流量	会话从建立开始到目前为止的发送流量和接收流量之和。

标题项	说明
创建时间	会话创建的时间。

1. 会话监控查询

会话监控下拉框查询，下拉选中某个字段，就会作为过滤条件，过滤出满足条件的所有会话信息。过滤条件有 TCP、UDP、ICMP、其它协议、组播、广播、全连接、半连接、本地连接、长连接、允许、拒绝、SNAT，DNAT。默认是无任何过滤条件的。会话时长超过半个小时的就标记为长连接。如图 2-19 所示，默认显示所有条件的会话信息。

图2-21 会话监控下拉框查询



搜索框查询，如图 2-22 所示。可以点击会话表中的某个或者某些字段，进行精确搜索；也可以输入关键字进行模糊搜索。

图2-22 搜索框查询

精确搜索可以点击：用户，用户组，源地址，目的地址，目的端口，协议，连接类型，应用。如图 2-23 所示，点击对应列就可以精确查询到相关会话信息。

图2-23 搜索框精确查询

模糊搜索匹配：用户，用户组，源地址，目的地址，协议，应用。如图 2-24 所示，直接在搜索框上输入查询关键字就能模糊匹配到相关会话信息。

图2-24 搜索框模糊查询

	用户	用户组	源地址	源端口	目的地址	目的端口	协议	类型	应用	发送流量	接收流量
1	10.1.2.2	匿名用户组	10.1.2.2	1977	180.163.238.164	80	TCP	全连接	网页浏览(HTTP)	5.51(KB)	9.17(KB)
2	10.1.2.2	匿名用户组	10.1.2.2	2817	36.110.231.11	80	TCP	全连接	网页浏览(HTTP)	163.53(KB)	88.87(KB)

2. 会话监控列展示

会话监控页面默认展示了常用的列，还有部分未进行展示，需要在会话监控页面任意标题列上有倒三角图标出现的时候点击倒三角就能选择未展示的列信息。如图 2-25 所示。

图2-25 选择会话监控列展示

点击倒三角之后，可以看到会话监控页面上会话相关的所有列，如图 2-26 所示。

图2-26 会话监控列选择

3 安全分析

3.1 安全分析简介

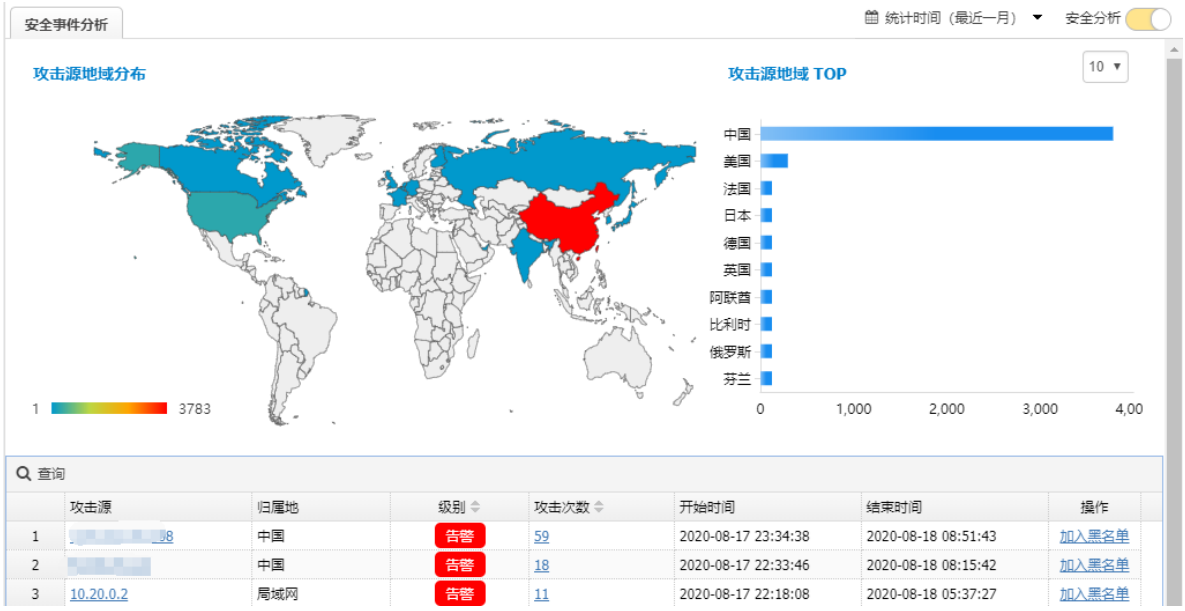
安全分析是对安全功能（IPS、AV、WEB 防护、安全防护、端口扫描）、资产等产生的数据进行统计分析，包括安全事件分析、资产安全分析和 WEB 防护分析。

- 安全事件分析以柱状图、地域分布图、表格形式展示攻击源信息。
- 资产安全分析以饼状图、表格形式展示资产 IP 信息。
- WEB 防护分析以柱状图、饼状图、趋势图形式分别展示规则防护和高级防护信息。

3.2 安全事件分析

在导航栏中选择“数据中心>安全分析>安全事件分析”进入安全事件分析页面，如图 3-1 所示。

图3-1 安全事件分析



对安全事件分析的详细说明如表 3-1 所示。

表3-1 用户流量说明

标题项	说明
统计时间	设定显示的时间跨度，可选的值有： • 最近一天 • 最近一周 • 最近一月 • 自定义时间 缺省情况下，显示最近一月的安全事件分析

标题项	说明
攻击源TOP	过滤显示TOP攻击源地址，可选的值有： • 10 • 50 缺省情况下，显示TOP10的攻击源
查询	点击查询，可以根据时间、级别、事件类型、攻击源、归属地、攻击目的进行组合查询
攻击源	显示攻击地址
归属地址	显示攻击地址所属归属地
级别	显示攻击源级别，且支持按照级别进行排序展示
攻击次数	显示攻击源攻击次数，且支持按照攻击次数进行排序展示
开始时间	攻击源第一次记录日志的时间
结束时间	攻击源最近一次记录日志的时间
操作	点击加入黑名单，可将此攻击源永久加入黑名单

点击“安全事件分析”表格里面的攻击源列里面的 IP 地址，进入对应攻击源详细统计的页面，如图 3-2 所示。

图3-2 单个攻击源详细统计

单个攻击源详细统计的详细说明如表 3-2 所示。

表3-2 单个用户流量统计说明

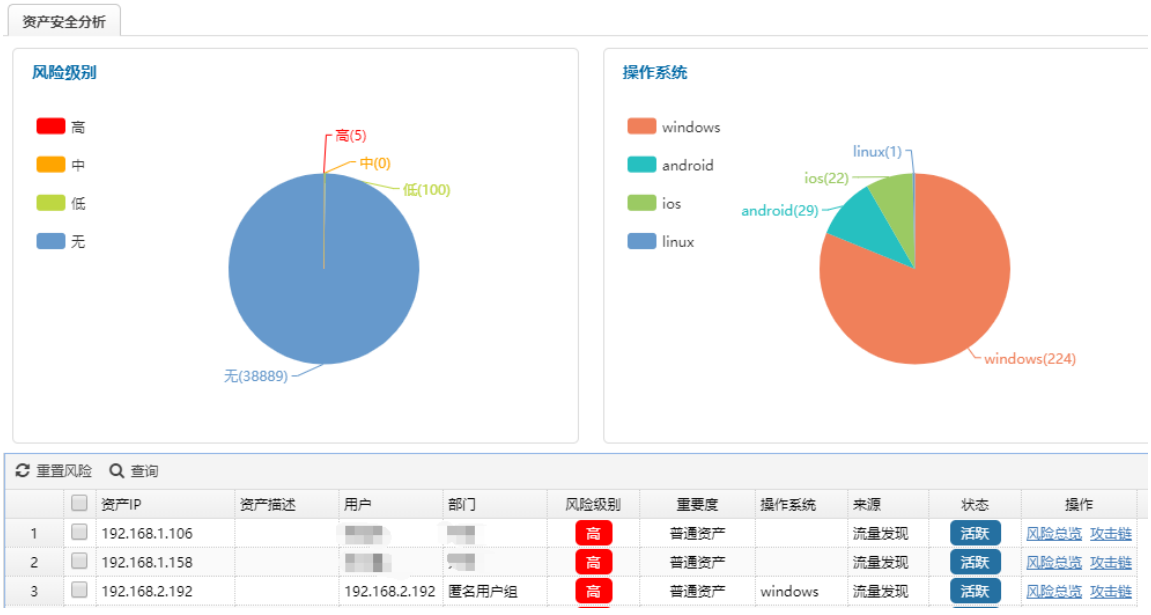
标题项	说明
统计时间	设定显示的时间跨度，可选的值有： • 最近一天 • 最近一周 • 最近一月 • 自定义时间

标题项	说明
	缺省情况下，显示自定义时间的攻击源详细统计
攻击链	点击不同阶段的攻击链，可以过滤展示此阶段产生的日志
查询	点击查询，可以根据时间、级别、事件类型、攻击源、归属地、攻击目的进行组合查询
时间	日志记录时间
级别	日志记录级别
攻击目的	被攻击地址
检测模块	攻击检测模块
事件类型	攻击日志所属的事件类型
事件名称	事件类型的描述
行为	显示此攻击的处理动作
操作	点击详细，展示详细的匹配信息和事件信息

3.3 资产安全分析

在导航栏中选择“数据中心>安全分析>资产安全分析”进入资产安全分析显示页面，如图 3-3 所示。

图3-3 资产安全分析



对资产安全分析的详细说明如表 3-3 所示。

表3-3 资产安全分析统计说明

标题项	说明
重置风险	支持单个或批量进行资产风险重置
查询	点击查询，可以根据资产IP、风险级别、资产描述、用户、部门、重要度、操作系统、状态进行组合查询
资产IP	资产IP地址
资产描述	资产的描述
用户	资产IP所属用户
部门	资产IP所属部门
风险级别	显示风险级别
重要度	显示资产的重要度
操作系统	显示资产的操作系统
来源	资产来源，有三种：流量发现、端口扫描、手工配置
状态	资产状态，活跃代表资产在线，空闲代表资产离线
操作	展示此资产的风险总览和攻击链

点击“资产安全分析”表格里面操作列的风险总览，进入对应风险总览显示的详细页面，如图 3-4 所示。

图3-4 风险总览显示页面

对风险总览详细信息的说明如表 3-4 所示。

表3-4 应用统计详细信息说明

标题项	说明
基本信息	展示资产IP、用户、部门、重要度、风险级别、操作系统和受攻击总数信息

标题项	说明
攻击趋势	以趋势图方式展示资产受不同类型攻击的趋势
攻击日志统计	以饼状图方式展示资产受不同类型攻击的占比
查询	点击查询，可以根据时间、级别、攻击者地址、事件来源、事件类型进行组合查询
攻击者地址	展示攻击者地址
归属地	攻击者地址所属地区
级别	攻击日志记录级别
事件类型	展示此资产被同一攻击者攻击而产生的攻击日志事件类型描述
事件条数	展示此资产被同一攻击者攻击而产生的攻击日志汇总条数
时间	展示此资产被同一攻击者攻击而第一条日志时间和最近一条日志的时间

点击“资产安全分析”表格里面操作列的攻击链，进入对应攻击链显示的详细页面，如图 3-5 所示。

图3-5 攻击链统计详细信息

对攻击链统计的详细说明如表 3-5 所示。

表3-5 单个应用流量统计说明

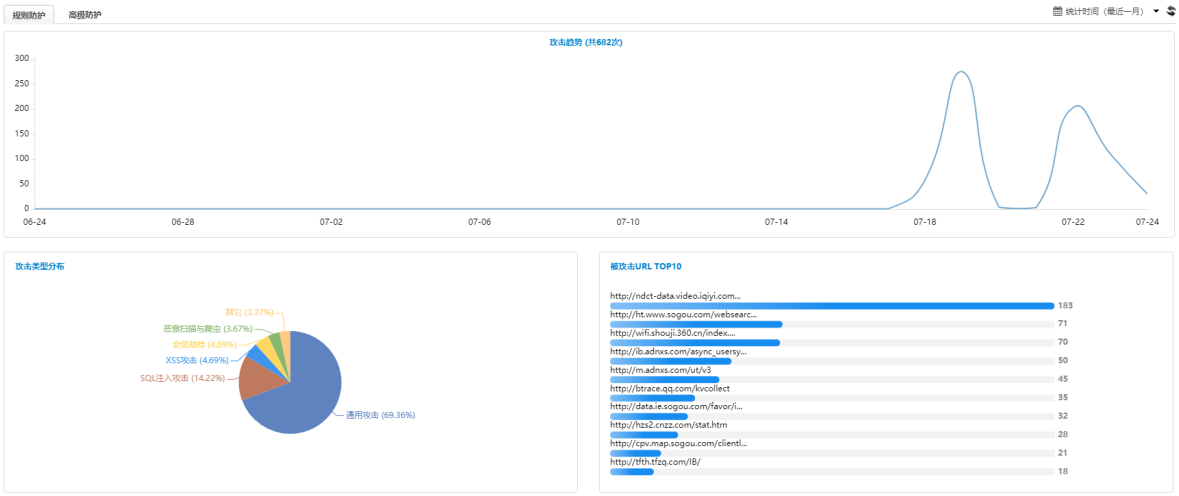
标题项	说明
攻击链	点击不同阶段的攻击链，可以过滤展示此阶段产生的日志
查询	点击查询，可以根据时间、级别、攻击源、事件来源、事件类型、事件名称进行组合查询
时间	日志记录时间
级别	日志记录级别
攻击源	攻击者地址
检测模块	攻击检测模块
事件类型	攻击日志所属的事件类型
事件名称	事件类型的描述

标题项	说明
行为	显示此攻击的处理动作
操作	点击详细，展示详细的匹配信息和事件信息

3.4 WEB防护分析

在导航栏中选择“数据中心>安全分析>WEB 防护分析”进入规则防护显示界面，如图 3-6 所示。

图3-6 规则防护



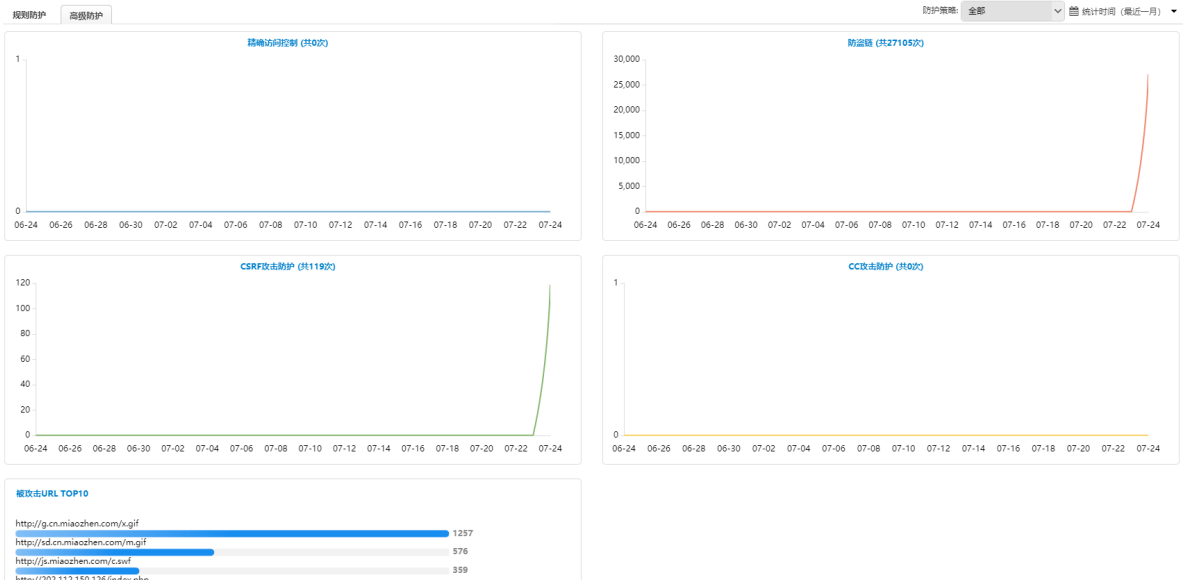
对规则防护的详细说明如表 3-6 所示。

表3-6 规则防护详细说明

标题项	说明
统计时间	设定显示的时间跨度，可选的值有： • 最近一天 • 最近一周 • 最近一月 • 自定义时间 缺省情况下，显示最近一月的规则防护统计
攻击类型分布	以饼状图的方式展示TOP5+其它的攻击类型占比
被攻击URL TOP10	以柱状图的方式展示TOP10的被攻击URL数据

在导航栏中选择“数据中心>安全分析>WEB 防护分析”进入规则防护显示界面，点击高级防护，进入高级防护显示页面，如图 3-7 所示。

图3-7 高级防护



对高级防护的详细说明如表 3-7 所示。

表3-7 高级防护详细说明

标题项	说明
防护策略	根据防护策略过滤展示数据，默认展示所有防护策略的数据
统计时间	设定显示的时间跨度，可选的值有： • 最近一天 • 最近一周 • 最近一月 • 自定义时间 缺省情况下，显示最近一月的高级防护统计
精确访问控制	以趋势图的方式展示精确访问控制策略命中趋势
防盗链	以趋势图的方式展示防盗链策略命中趋势
CSRF攻击防护	以趋势图的方式展示CSRF攻击防护策略命中趋势
CC攻击防护	以趋势图的方式展示CC攻击防护策略命中趋势
被攻击URL TOP10	以柱状图的方式展示TOP10的被攻击URL数据

目 录

1 U 盘零配置启动 1-1
1.1 概述 1-1
1.2 使用方法 1-1
1.2.1 使用前准备 1-1
1.2.2 制作启动 U 盘 1-2
1.2.3 后续配置 1-3

1 U 盘零配置启动

1.1 概述

设备初始安装时通常需要预先进行配置才能上线。传统上此项业务主要交由实施人员手工进行配置。但此种上线模式主要适合小规模安装，并容忍一定的人为出错几率。而对于较大型的项目，需要实施的网点多，手工配置的方式则较为费时费力，安装和实施成本较高。因此需要支持通过 U 盘进行零配置上线的方案。

具体流程如下：

(1) 设备在启动过程中判断 U 盘根目录是否有文件名为“ausbsetup.tst”的文件，有表示该盘是零配置启动盘，没有则表示该盘非零配置启动盘；

(2) 当确认是零配置启动盘之后，需要设备根据自己的软件序列号，查找该零配置启动盘上是否有按照自己软件序列号命名的文件夹；

(3) 如果有以自己软件序列号命名的文件夹，则读取改文件夹下的 version 文件，从中获取需要升级的版本号和需要升级的 bin 文件；

(4) 通过设备上运行的版本号和读取到的版本号判断是否需要升级，版本号相同则不需要升级，版本号不同则需要升级；

(5) 根据需要升级的 bin 文件名到 U 盘根目录下的 version 文件夹中获取需要升级的 bin 文件，获取到 bin 文件后开始正常的升级流程；

(6) 设备版本升级完成之后继续执行配置的导入，将与设备序列号一致的文件夹中名为 startup-config-u.cfg 的文件作为设备启动后默认运行的配置导入到设备中；为了配置的安全性考虑，配置文件是经过加密处理的，具体的加密方式是将文件内容以字节为单位进行高低位互换以达到加密的目的；

(7) 目前设备还支持备份配置的导入，其在设备序列号命名的文件夹下，有一个 backup-conf 命名的文件夹，里面存放是设备备份配置信息，设备在零启动过程中可以将其作为备份配置信息导入，最多可以导入三份备份文件；

(8) U 盘零配置启动完成，需要在设备序列号命名的文件夹下创建一个名 finish.txt 的文件，以便标志本次零配置启动完成，从而避免了设备反复运行零启动过程。

1.2 使用方法

1.2.1 使用前准备

使用前，请先准备 U 盘并收集设备的信息。

(1) 准备一个 FAT32 格式空 U 盘，品牌不限。

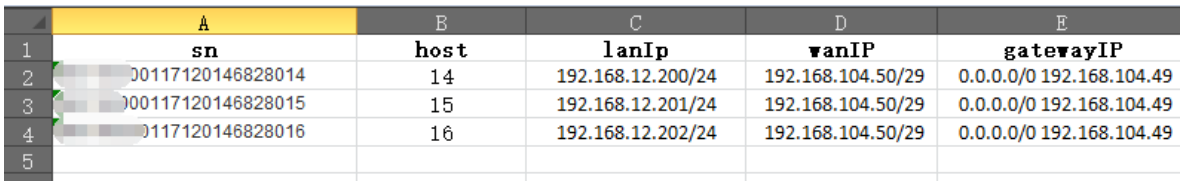
(2) 准备需要升级的目标软件版本。

(3) 收集设备的软件序列号以及内外网接口信息。

1.2.2 制作启动 U 盘

(1) 创建一个名称为 param.xlsx 的文件，并将收集的设备软件序列号和基础配置填写到表格中保存。

图1-1 创建 param.xlsx



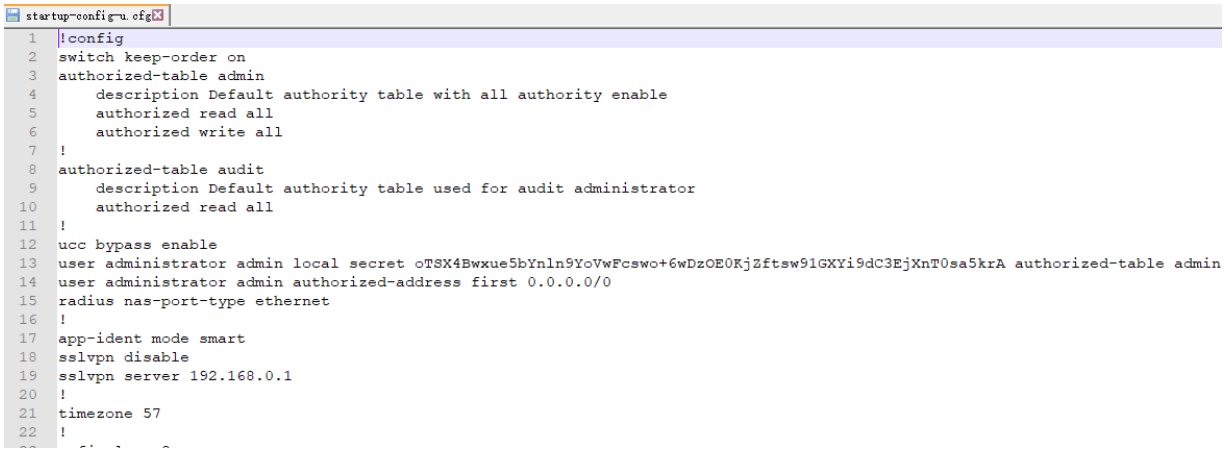
	A	B	C	D	E
1	sn	host	lanIp	wanIP	gatewayIP
2	[redacted]00117120146828014	14	192.168.12.200/24	192.168.104.50/29	0.0.0.0/0 192.168.104.49
3	[redacted]000117120146828015	15	192.168.12.201/24	192.168.104.50/29	0.0.0.0/0 192.168.104.49
4	[redacted]0117120146828016	16	192.168.12.202/24	192.168.104.50/29	0.0.0.0/0 192.168.104.49
5					

表1-1 参数说明

参数	说明
sn	设备的软件序列号，可以通过设备后面板的sn标签获取。
host	主机名称，用于修改对应的设备主机名称。
lanIp	设置内网口IP地址（预留项，目前无实际意义）。
wanIP	外网口IP地址（预留项，目前无实际意义）。
gatewayIP	默认网关地址，用于生成默认路由（预留项，目前无实际意义）。

(2) 创建配置文件。新建一个 startup-config-u.cfg 文件，并使用文本编辑。从命令行中将已经配置好的配置通过 show current-config 命令将配置文件复制粘贴到 startup-config-u.cfg 中，并保存配置。

图1-2 编辑 startup-config-u.cfg 文件



startup-config-u.cfg

```
!config
switch keep-order on
authorized-table admin
    description Default authority table with all authority enable
    authorized read all
    authorized write all
!
authorized-table audit
    description Default authority table used for audit administrator
    authorized read all
!
ucc bypass enable
user administrator admin local secret oTSX4Bwxue5bYnln9YoVwFcswo+6wDzOE0KjZftsw91GXYi9dC3EjXnT0sa5krA authorized-table admin
user administrator admin authorized-address first 0.0.0.0/0
radius nas-port-type ethernet
!
app-ident mode smart
sslvpn disable
sslvpn server 192.168.0.1
!
timezone 57
!
```

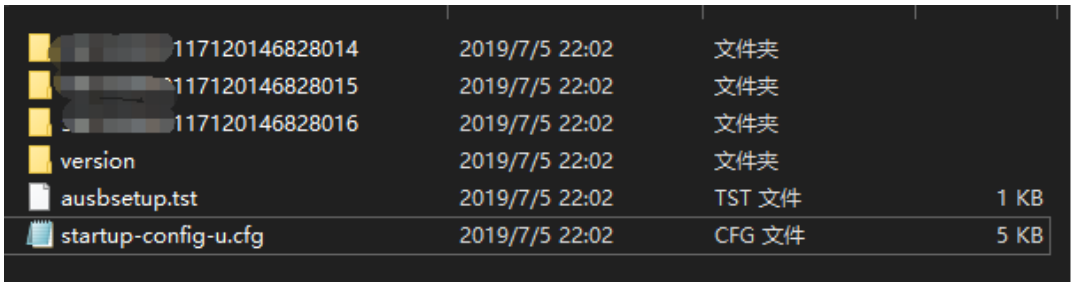
(3) 使用 U 盘配置文件生成软件生成相关的数据，请准备好 param.xlsx、startup-config-u.cfg 及需要升级的目标软件版本，并联系技术工程师生成。

(4) 在生成的数据文件中，进入 datas 目录，可以看到有一个一串数字的文件夹，该文件夹下有两个子文件夹 CommonData 和 UData。其中 CommonData 保存配置文件替换后的普通数据未加密，用于配置备份，Udata 作为 U 盘根目录，保存加密的配置文件。

图1-3 生成的文件夹

UData 目录下又有以软件序列号命名的文件夹、version 文件夹、ausbsetup.tst 文件以及 startup-config-u.cfg 文件。

图1-4 UData 目录



(5) 将 UData 文件夹拷贝至 U 盘的根目录下。此时，启动 U 盘制作完成。

2. 使用启动 U 盘

(1) 设备加电前，将启动 U 盘插入设备的 USB 接口，加电启动。

(2) 设备自动识别 U 盘中的内容，找到与自身一致的序列号文件夹进行版本升级和配置替换，并在替换完成后在该文件夹中写入 finish.txt、upgrade_finish.txt 文件。

(3) 设备启动运行时即为目标软件版本以及配置。

1.2.3 后续配置

如果后续需要针对该设备再次上线，可以将其对应的文件夹下的 finish.txt、upgrade_finish.txt 文件删除。然后再根据使用启动 U 盘进行配置。

目 录

1 统计报表 ····· 1-1
1.1 简介 ····· 1-1
1.2 报表管理 ····· 1-1
1.3 数据统计 ····· 1-4
1.4 配置管理 ····· 1-4
1.4.1 报表配置 ····· 1-4
1.4.2 IPS 业务系统管理 ····· 1-6
1.5 报表管理配置举例 ····· 1-8
1.5.1 报表管理配置举例 ····· 1-8

1 统计报表

1.1 简介

统计报表模块可以对设备健康状态、用户上网行为、网络质量、网络安全不同维度进行统计，将统计的数据以报表的格式定时生成发送给管理员。统计报表主要包括报表管理、数据统计、配置管理三大模块。

- 报表管理主要配置报表任务并查看历史报表信息。
- 数据统计主要对用户上网审计相关行为数据进行统计。
- 配置管理主要对报表中使用磁盘管理以及报表管理相关参数进行设置。

1.2 报表管理

通过菜单“数据中心 > 统计报表 > 报表管理”，进入如图 1-1 所示页面。在该页面上可以配置报表任务的相关功能。

图1-1 报表管理页面

报表管理详细说明如表 1-1 所示。

表1-1 报表管理详细说明

标题项	说明
名称	创建报表任务的名称。
状态	状态有启用和禁用两种： 表示启用； 表示禁用。
创建时间	创建报表任务的时间。
历史报表	报表任务生成的历史报表，点击数字可直接跳转到历史报表中查看具体生成的历史报表。
报表类型	报表类型有日报表、周报表、月报表、单次报表四种类型。
统计时间	生成报表汇聚数据的时间范围。
报表格式	报表格式支持HTML和PDF两种格式。
外发方式	外发方式支持FTP和邮件两种方式，邮件外发设备上需要配置DNS服务器地址；两者都不选，则不外发。

点击<新建>按钮，可以按需求创建报表任务，如图 1-2 所示。

图1-2 新建报表任务

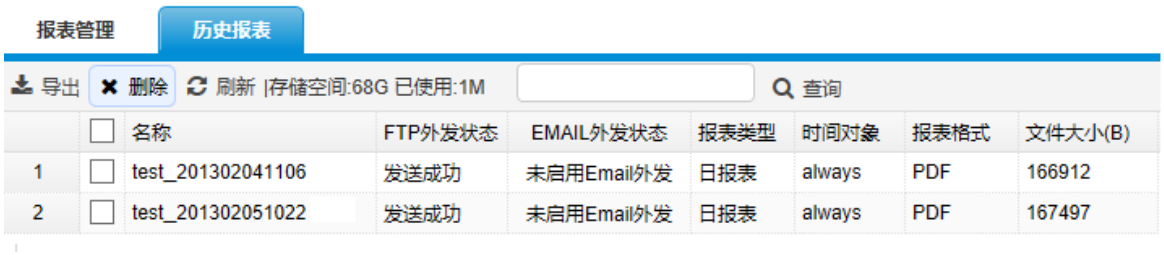
新建报表任务详细说明如表 1-2 所示。

表1-2 新建报表任务详细说明

标题项	说明
是否启用	创建的报表任务是否启用，勾选表示启用，不勾选表示禁用。
报表名称	创建报表任务的名称。
报表类型	报表类型主要包括日报表、周报表、月报表、单次报表四种类型。 • 日报表：每天汇聚统计生成一个报表； • 周报表：每周汇聚统计生成一个报表； • 月报表：每月汇聚统计生成一个报表； • 单次报表：按指定统计时间生成一个报表。
统计时间	生成报表汇聚数据的时间范围。
报表格式	报表格式支持HTML和PDF两种格式。
外发方式	外发方式支持FTP和邮件两种方式，邮件外发设备上需要配置DNS服务器地址；两者都不选，则不外发。
外发后删除	报表外发成功之后，将本地生成的历史报表删除，减少磁盘占用空间，如果同时配置了FTP和邮件外发，其中一个外发失败，将不会删除该报表对应生成的历史报表。
外发邮箱	收件邮箱地址，最多配置32个，多个邮箱用换行区分。
报表模板	自定义报表模板需要根据需求选择下面的订阅项目； 预定义模板，主要包括网络概况、工作效率、数据统计三大模板。

通过菜单“数据中心>统计报表>报表管理>历史报表”，进入如图 1-3 所示页面，在该页面上可以查看已经生成的历史报表。

图1-3 历史报表



历史报表参数详细说明如表 1-3 所示。

表1-3 历史报表详细说明

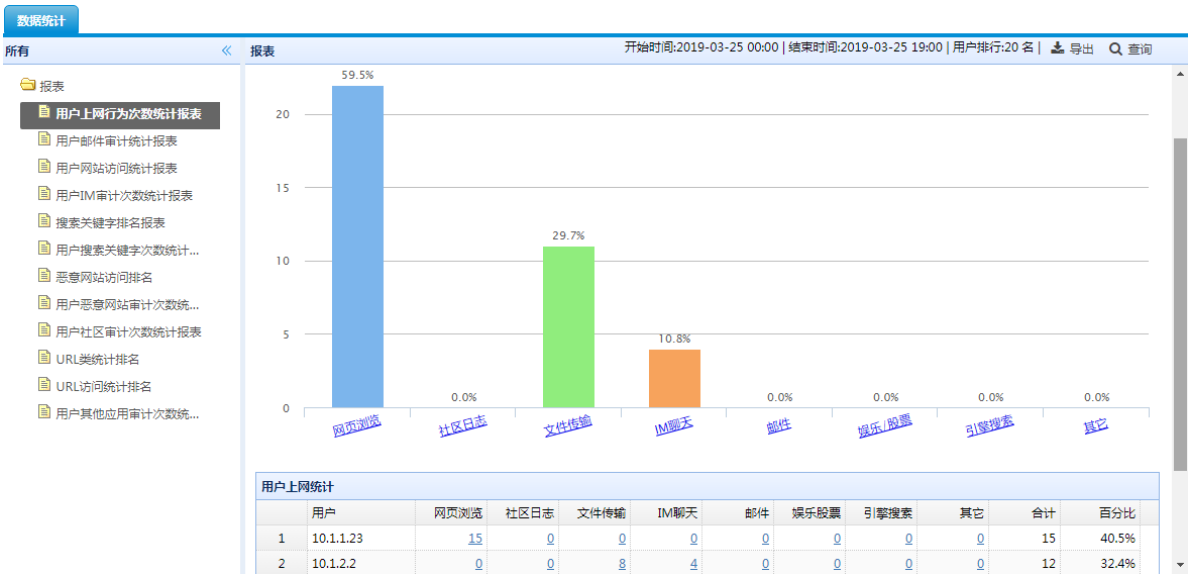
标题项	说明
名称	生成报表的名称，以创建报表任务名称+生成报表的时间组合生成。
FTP外发状态	配置FTP外发，状态有发送成功，发送失败两种。 不配置FTP外发，状态显示为未启用FTP外发。
EMAIL外发状态	配置邮件外发，状态有发送成功，发送失败两种。 不配置邮件外发，状态显示为未启用Email外发。

报表类型	报表类型有日报表、周报表、月报表、单次报表四种类型。
时间对象	生成报表汇聚数据的时间范围。
报表格式	报表格式支持HTML和PDF两种格式，1G内存设备只支持HTML格式。
文件大小	生成报表文件的大小，以字节为单位。

1.3 数据统计

通过菜单“数据中心 > 统计报表 > 数据统计”，进入如图 1-4 所示页面。在该页面上可以查看用户上网行为各项数据统计。该数据统计依赖于 IPv4 审计策略，主要由内网用户访问外网时上网行为的统计数据汇聚而成。

图1-4 数据统计



数据统计以上网行为维度和用户维度分别进行统计数据，以上网行为维度统计数据通过柱状图显示，以用户维度统计数据通过列表方式显示。

1.4 配置管理

1.4.1 报表配置

通过菜单“数据中心 > 统计报表 > 配置管理”，进入如图 1-5 所示页面。在该页面上配置磁盘管理和报表管理相关参数项。

图1-5 报表配置管理页面

报表配置管理页面详细参数说明如表 1-4 所示。

表1-4 报表配置管理页面详细说明

标题项	说明
数据采集	开启/关闭数据统计，系统默认为关闭，配置报表后会自动开启。
报表空间	报表模块所使用的磁盘空间大小，推荐不超过磁盘空间的15%。
报表归档	报表阈值大小，当报表文件总体大小达到报表空间设置大小的归档百分比之后，将会删除最开始生成的历史报表文件，删除报表文件数减少到小于归档值之后不再删除。
报表排名用户数	报表任务中对用户数排名默认统计TOP50的用户数据，根据需求修改，最大配置300。

标题项	说明
周起始日	此项仅对周报表任务有效，周起始日默认以周日开始。

1.4.2 IPS 业务系统管理

系统可以根据配置的业务系统和内容生成 IPS 网络安全分析报表，通过对业务和用户的受攻击、威胁情况进行统计分析，为用户提供详细、多维度的安全分析统计报告。报表内容包括威胁分布、攻击趋势、攻击源 TOP、攻击目的 TOP、日志级别分布、IPS 事件 TOP、攻击协议分布。

针对业务系统的安全分析就是对发生在该业务系统的网络范围内的攻击进行统计分析，输出报表。IPS业务系统管理用于配置网络中业务系统和IP的对应关系，可以对内网区域进行标识和逻辑划分，针对每个业务系统输出报表，内容包括排名、业务系统、攻击次数、占比等。

一个业务系统可以是一个或者多个 IP 网段，同一个报表任务中的不同业务系统 IP 不可冲突。

1. IPS 业务系统管理页面

通过菜单“数据中心 > 统计报表 > 配置管理 > IPS 业务系统管理”，即可进入 IPS 业务系统管理配置界面，配置 IPS 业务系统信息，如图 1-6 所示。

图1-6 IPS 业务系统管理页面

IPS 业务系统管理参数说明如表 1-5 所示。

表1-5 IPS 业务系统管理参数说明

参数	说明
创建时间	创建IPS业务系统管理配置策略的时间.
业务系统名称	创建IPS业务系统管理配置的名称.
业务系统IP	创建IPS业务系统管理配置添加的IP地址.
是否使用	IPS业务系统被报表任务引用的状态，被引用显示已使用，未引用则显示未使用。
操作	此项仅对未引用的IPS业务系统进行编辑操作。

2. 新建 IPS 业务系统

单击“新建”按钮，可以创建 IPS 业务系统，如图 1-7 所示。

图1-7 新建 IPS 业务系统管理

表1-6 新建 IPS 业务系统管理配置参数说明

参数	说明
业务系统名称	创建IPS业务系统管理配置的名称。
业务系统IP	创建IPS业务系统管理配置添加的IP地址，IP地址格式支持：子网地址、范围地址和主机地址三种。
已添加项目	已添加的IP地址。

3. 配置报表

通过菜单“数据中心 > 统计报表 > 报表管理”，进入报表管理页面，新建或编辑管理报表，选择“自定义报表模板”，在订阅项目中单击选择“IPS 网络安全分析”，弹出“IPS 网络安全分析”界面，如图 1-8 所示。勾选“业务系统分布”，单击“请选择业务系统”，选择要生成报表的业务系统，如图 1-9 所示。单击 “提交” 按钮完成配置。

图1-8 设置 IPS 网络安全分析报表

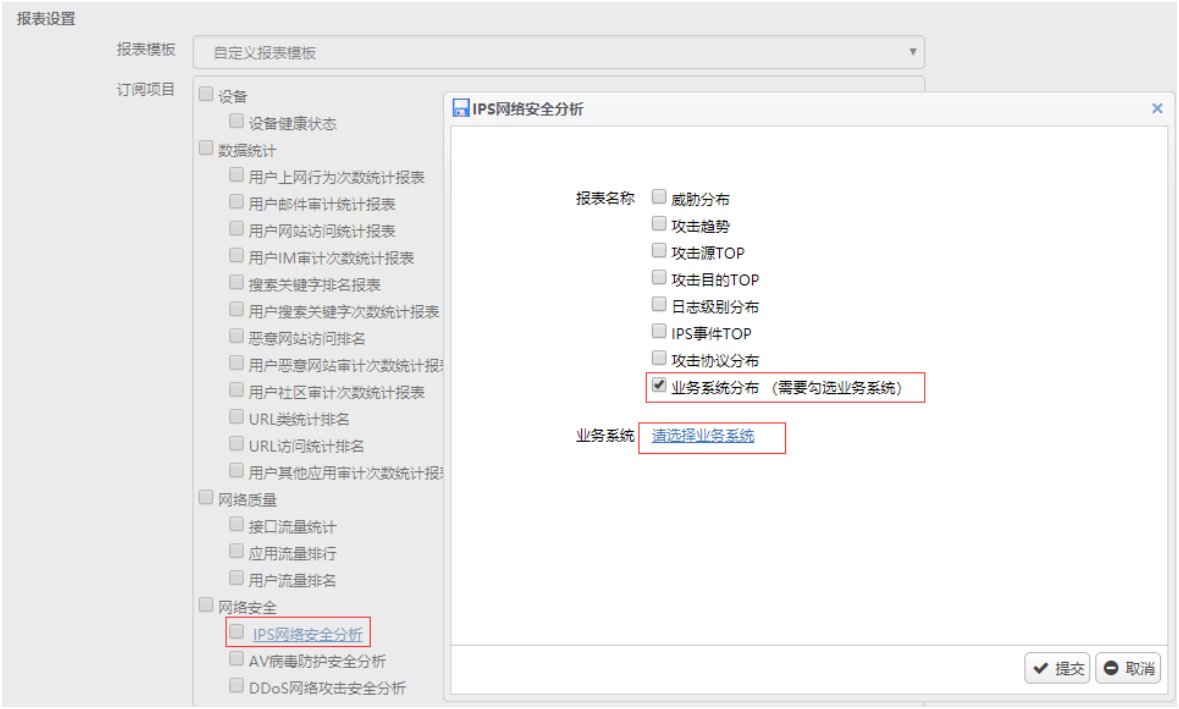
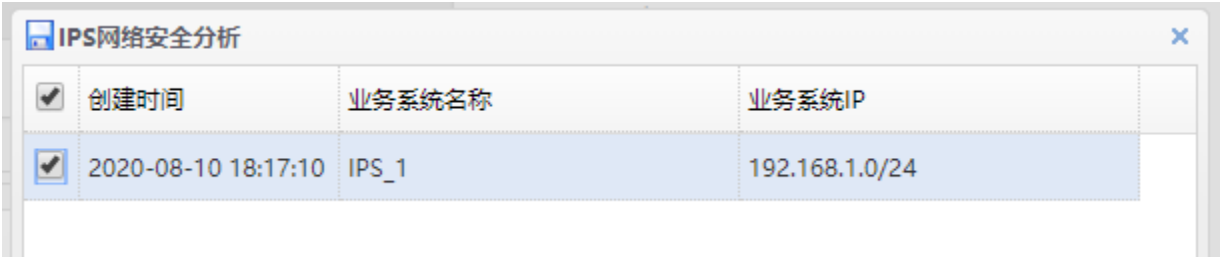


图1-9 选择 IPS 业务系统



1.5 报表管理配置举例

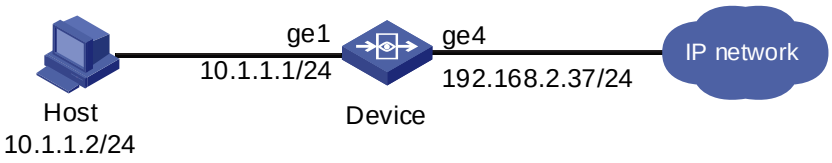
1.5.1 报表管理配置举例

1. 组网需求

- 内网用户过设备访问外网，对内网访问外网的上网行为进行审计，并要求每日生成报表。
- 设备能够与外网通信。

2. 组网图

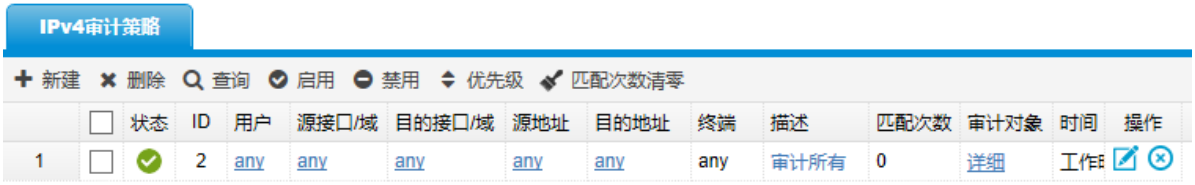
图1-10 统计报表组网图



3. 配置步骤

(1) 配置 IPv4 审计策略。如图 1-11 所示。

图1-11 配置 IPv4 审计策略



(2) 配置报表任务。如图 1-12 所示。

图1-12 报表管理页面

(3) 配置 FTP 服务器，进入系统管理>服务器管理>FTP 服务器页面，配置 FTP 服务器，如图 1-13 所示。

图1-13 FTP 服务器配置

配置邮件服务器，进入系统管理>服务器管理>邮件服务器页面，设置发送邮件服务器信息，如图 1-14 所示。

图1-14 邮件服务器配置

配置 DNS 服务器，进入网络管理>DNS 服务>DNS 服务器页面，配置 DNS 服务器地址。如图 1-15 所示。

图1-15 DNS 服务器配置

4. 验证配置

配置完成后，内网用户通过设备上网的行为被设备审计，且报表模块可以根据上网行为审计数据进行统计如图 1-16 所示，并生成对应的日报表如图 1-17 所示。

图1-16 数据统计

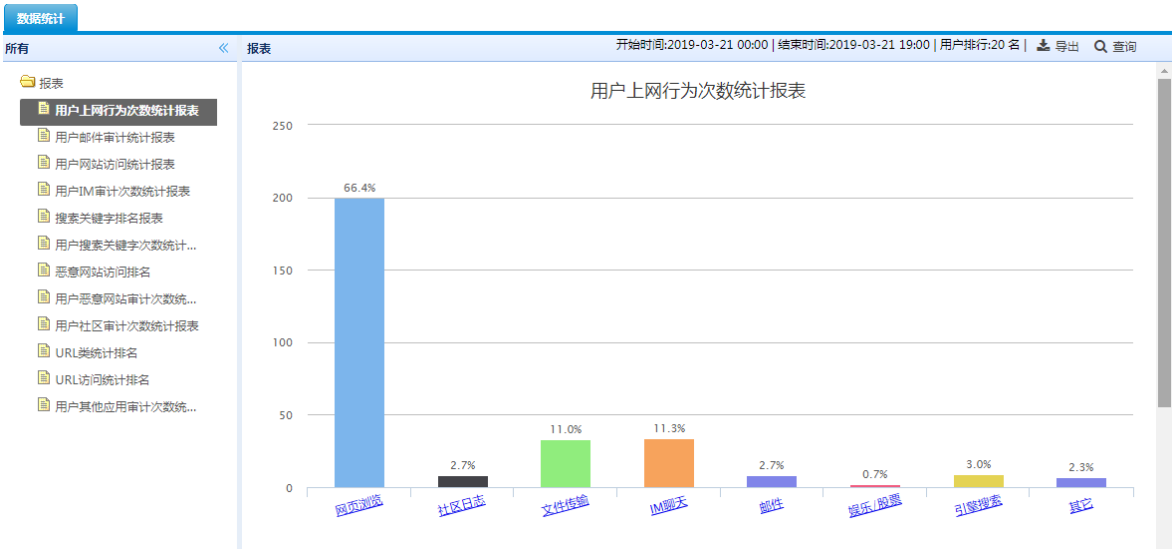


图1-17 生成的历史报表

说明

- 配置报表邮件外发时，设备必须能够与外网通信，且需要配置 DNS 服务器地址。
- 1G 内存设备报表格式只支持 HTML 格式，2G 及 2G 内存以上设备报表格式支持 HTML 和 PDF 两种格式。
- 数据统计按小时进行整点汇聚，汇聚的数据与审计模块统计的数据可能存在小范围的误差。
- 报表上网行为统计以及数据统计依赖于 IPv4 审计策略，如果不配置 IPv4 审计策略，此项统计将为空。

目 录

1 接口配置 ····· 1-1
1.1 以太网接口配置 ····· 1-1
1.1.1 概述 ····· 1-1
1.1.2 接口显示 ····· 1-1
1.1.3 接口修改 ····· 1-2
1.1.4 接口 IPv4 地址配置 ····· 1-4
1.1.5 接口 IPv6 地址配置 ····· 1-5
1.1.6 以太网接口配置举例 ····· 1-8
1.2 VLAN 接口配置 ····· 1-9
1.2.1 VLAN 概述 ····· 1-9
1.2.2 VLAN 接口创建 ····· 1-10
1.2.3 VLAN 接口显示 ····· 1-11
1.2.4 VLAN 接口修改 ····· 1-11
1.2.5 VLAN 接口删除 ····· 1-12
1.3 桥接口配置 ····· 1-12
1.3.1 桥接口概述 ····· 1-12
1.3.2 桥接口创建 ····· 1-13
1.3.3 桥接口显示 ····· 1-14
1.3.4 桥接口修改 ····· 1-14
1.3.5 桥接口删除 ····· 1-15
1.4 聚合接口配置 ····· 1-15
1.4.1 接口聚合概述 ····· 1-15
1.4.2 聚合接口创建 ····· 1-15
1.4.3 聚合接口显示 ····· 1-17
1.4.4 聚合接口修改 ····· 1-17
1.4.5 聚合接口删除 ····· 1-18
1.5 隧道接口配置 ····· 1-18
1.5.1 隧道接口概述 ····· 1-18
1.5.2 隧道接口创建 ····· 1-18
1.5.3 隧道接口显示 ····· 1-18
1.5.4 隧道接口修改 ····· 1-19
1.6 无线接口配置 ····· 1-20
1.6.1 无线接口概述 ····· 1-20

1.6.2 无线接口创建 ····· 1-20
1.6.3 无线接口显示 ····· 1-20
1.6.4 无线接口修改 ····· 1-20
1.7 配置安全域 ····· 1-22
1.7.1 背景信息 ····· 1-22
1.7.2 安全域创建 ····· 1-22
1.7.3 安全域显示 ····· 1-23
1.7.4 安全域修改 ····· 1-23
1.7.5 安全域删除 ····· 1-23
1.8 配置虚拟网线 ····· 1-23
1.8.1 背景信息 ····· 1-23
1.8.2 虚拟网线创建 ····· 1-24
1.8.3 虚拟网线显示 ····· 1-24
1.8.4 虚拟网线修改 ····· 1-25
1.8.5 虚拟网线删除 ····· 1-25
1.9 VLAN 接口，桥接口，聚合接口创建及交互举例 ····· 1-25
1.10 配置 IPv6 隧道接口 ····· 1-28
1.10.1 隧道技术概述 ····· 1-28
1.10.2 IPv6 隧道接口创建 ····· 1-29
1.10.3 IPv6 隧道接口修改 ····· 1-30
1.10.4 IPv6 隧道接口删除 ····· 1-31
1.10.5 IPv6 隧道接口属性配置 ····· 1-31
1.10.6 IPv6 隧道接口配置举例 ····· 1-32
1.11 配置 IPsec 隧道接口 ····· 1-34
1.11.1 IPsec 隧道接口创建 ····· 1-34
1.11.2 IPsec 隧道接口修改 ····· 1-35
1.11.3 IPsec 隧道接口删除 ····· 1-36
1.11.4 IPsec 隧道接口属性配置 ····· 1-36
1.11.5 IPec 隧道接口配置举例 ····· 1-37

1 接口配置

1.1 以太网接口配置

1.1.1 概述

表1-1 以太网接口缺省配置

内容	缺省设置	备注
端口自协商配置	on	可以更改设置
端口MTU	1500	可以更改设置
端口管理状态	no shutdown	可以更改设置

说明

- 物理接口在设备启动的时候就已经创建，不支持在设备运行过程中创建或者删除。
- 可以通过修改以太网的端口的配置来改变物理接口的运行方式。

1.1.2 接口显示

如图 1-1所示，点击导航栏中的“网络配置 > 接口配置 > 物理接口”，进入物理接口的显示界面。

图1-1 物理接口显示界面

物理接口 | 子接口 | 网桥接口 | 聚合接口 | 隧道接口 | 无线接口 | 安全域 | 虚拟网线

	接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1	ge0		192.168.100.2/24		60:0b:03:ad:24::	route	full	1000	down		
2	ge1				60:0b:03:ad:24::	route	full	1000	down		
3	ge2		172.16.11.1/24		60:0b:03:ad:24::	route	full	1000	down		
4	ge3				60:0b:03:ad:24::	route	full	1000	down		
5	ge4				60:0b:03:ad:24::	route	full	1000	down		
6	ge5				60:0b:03:ad:24::	route	full	1000	down		
7	ge6				60:0b:03:ad:24::	route	full	1000	down		
8	ge7				60:0b:03:ad:24::	route	full	1000	down		
9	ge8				60:0b:03:ad:24::	route	full	1000	down		
10	ge9				60:0b:03:ad:24::	switch	full	100	up		
11	ge10				60:0b:03:ad:24::	switch	full	100	up		

表1-2 物理接口显示界面详细描述表

配置项	说明
接口名称	物理接口名称

配置项	说明
描述	接口描述
IP地址	接口的IP地址/掩码，可以通过静态配置、DHCP、PPPoE获取
IPv6地址	接口的IPv6地址/前缀长度，可以在页面上手工配置
MAC地址	该接口对应的MAC地址
工作模式	接口工作模式，包括route、switch、agged、vline、listen
双工模式	设置端口双工工作模式，有全双工和半双工两种模式
速率	接口支持的数据传输速率
连接状态	接口的连接状态
启用状态	接口是否被启用
操作	对该接口进行编辑

1.1.3 接口修改

点击图 1-2 物理口显示界面中，对应接口下的<编辑>按钮，显示配置界面。

图1-2 物理口配置界面

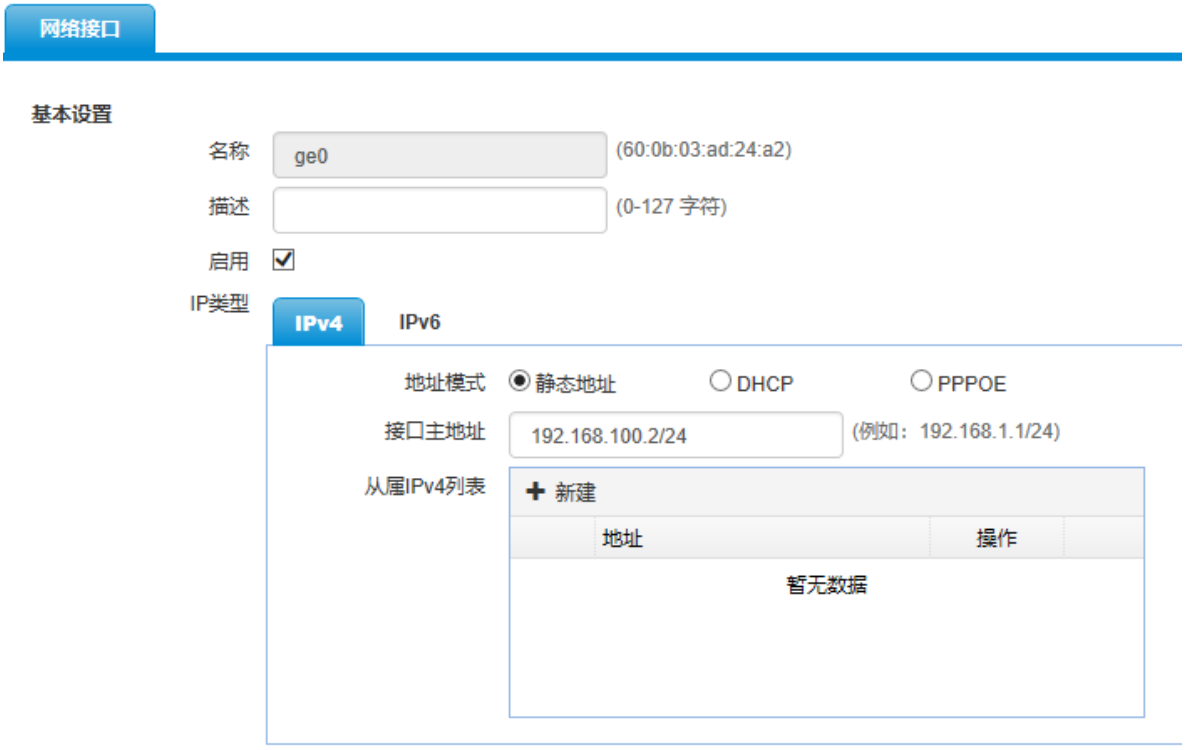


表1-3 物理接口配置详细描述表

配置项	说明
名称	物理接口名称
描述	接口描述
启用	物理接口的管理状态，勾选时启用，不选时接口关闭
IP类型	IPv4地址和IPv6地址；点击相应的标签，配置对应类型的IP地址
地址模式	对于IPv4地址，有三种获取模式，分别为静态配置、DHCP和PPPoE； 对于IPv6地址，有四种获取模式，分别为静态配置、DHCP、PPPOE和NDRA。

图1-3 物理口高级配置界面

表1-4 物理接口高级配置详细信息描述表

配置项	说明
管理方式	配置端口是否允许 HTTPS、HTTP、SSH、Telnet、Ping、Center-monitor 等管理服务
协商模式	分为自协商和非自协商两种方式： • 自协商模式下，端口的所有参数都是自动协商出来的，不能设置端口的速率和双工模式参数 • 强制模式下，可以设置端口的速率和双工模式，双方端口的参数设置必须一致，否则会导致端口工作不正常，造成端口不通或者丢包等问题
速率	设置端口速率，百兆端口可以设为10/100，千兆端口可以设为10/100/1000，只能在强制模式下使用
双工模式	设置端口双工工作模式，有全双工和半双工两种模式
MTU	接口发送报文的最大长度，缺省为1500，单位为字节
接口属性	内网口：组网的内部接口 外网口：组网与外网交互的接口

1.1.4 接口 IPv4 地址配置

接口的 IPv4 地址有三种模式的配置方式，分别为静态配置、DHCP 和 PPPoE，通过菜单“网络配置 > 接口配置 > 物理接口”进入物理界面显示界面，点击对应接口后面的编辑图标进入物理口配置页面。

下面分别介绍：

1. 静态配置

IPv4 地址/掩码：静态配置的 IP 地址和掩码（包括主 ip 和 secondary ip）。配置页面见图 1-2。

2. DHCP 模式

切换 IPv4 地址模式为 DHCP，可进入 DHCP 配置页面，如图 1-4 所示。如选择 DHCP 模式，则接口作为 DHCP 客户端经由 DHCP 服务器获取地址。

图1-4 DHCP 配置界面

表1-5 配置说明

配置项	说明
优先级	配置DHCP优先级<1~255>
DHCP属性	选择是否更新网关或更新DNS

3. PPPoE

即配置接口作为 PPPoE 客户端。PPPoE 是 Point-to-Point Protocol over Ethernet 的简称，它利用以太网将大量主机组成网络，通过一个远端接入设备连入因特网，并对接入的每个主机实现控制、计费功能，极高的性能价格比使 PPPoE 在包括小区组网建设等一系列应用中被广泛采用。

图1-5 PPPoE 配置界面

表1-6 PPPoE 详细信息描述表

配置项	说明
用户名	PPPoE拨号的用户名
密码	PPPoE拨号的密码
优先级	配置PPPoE优先级<1~255>
PPPoE属性	选择是否更新网关或更新DNS

1.1.5 接口 IPv6 地址配置

接口的 IPv6 地址有四种模式的配置方式，分别为静态配置、DHCP、PPPOE 和 NDRA，通过菜单“网络配置 > 接口配置 > 物理接口”进入物理接口显示界面，点击对应接口后面的编辑图标进入物理口配置页面，IP 类型选择“IPv6”页签，进入接口的 IPv6 地址配置页面。

1. IPv6 静态地址配置

进入物理接口配置页面，切换 IP 类型为 IPv6，进入 IPv6 静态地址配置页面。

图1-6 接口 IPv6 静态地址配置界面

表1-7 IPv6 静态地址详细信息描述表

配置项	说明
地址模式	支持四种模式，分别为静态配置、DHCP、PPPOE和NDRA。
接口主地址	IPv6地址/前缀长度，主地址概念同IPv4相同。
从属IPv6列表	点击<新建>按钮，可以添加从IPv6地址。

2. IPv6 DHCP 模式

切换 IPv6 地址模式为 DHCP，进入 IPv6 DHCP 配置页面，如下图所示。如选择 DHCP 模式则接口作为 DHCP 客户端经由 DHCP 服务器获取地址。

图1-7 IPv6 DHCP 配置界面

3. IPv6 PPPoE

切换 IPv6 地址模式为 PPPoE，进入 IPv6 PPPoE 配置页面，如下图所示。如选择 PPPoE 模式则接口作为 PPPoE 客户端经由 PPPoE 服务器获取地址。

图1-8 IPv6 PPPoE 配置界面

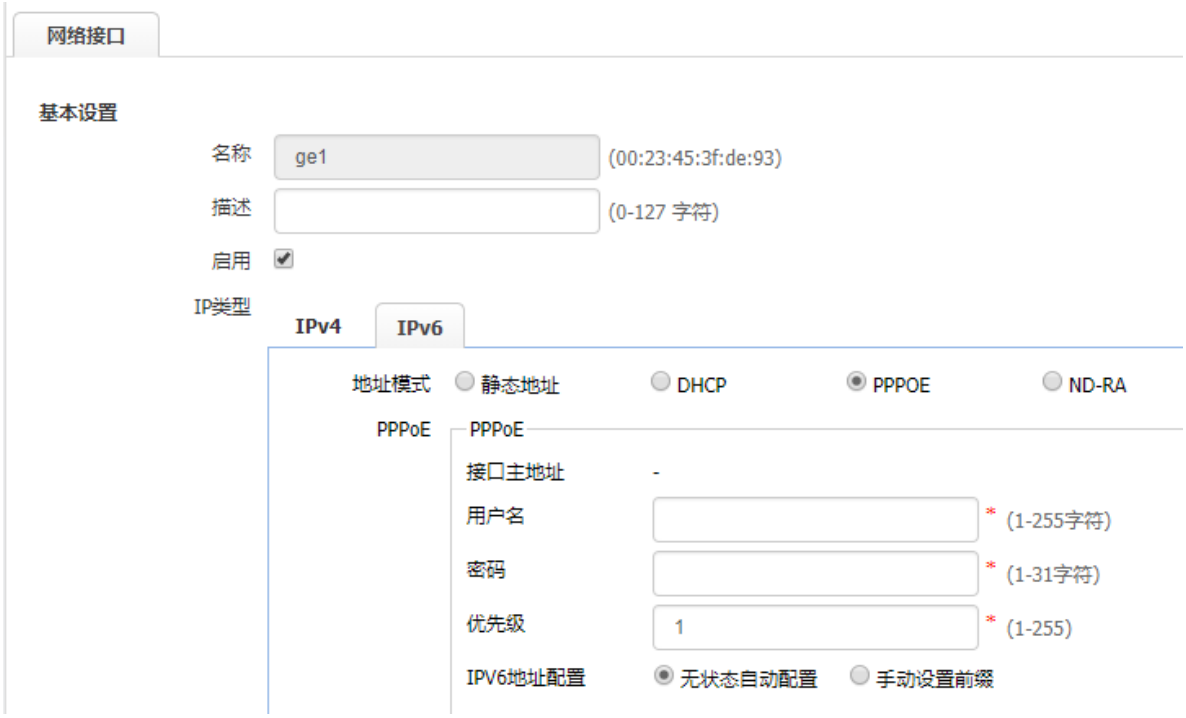


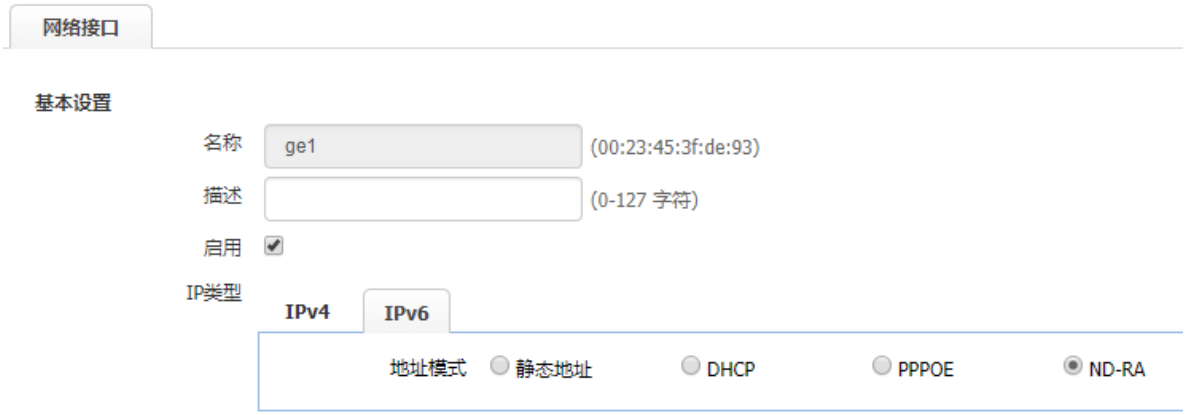
表1-8 IPv6 PPPoE 地址详细信息描述表

配置项	说明
接口主地址	经由PPPoE服务器获取的地址。
用户名	PPPoE拨号的用户名。
密码	PPPoE拨号的密码。
优先级	配置PPPoE优先级<1~255>。
IPv6地址配置	选择无状态自动配置可以从PPPoE服务器获取前缀，并通过EUI64计算出接口ID。

4. IPv6 NDRA 模式

切换 IPv6 地址模式为 NDRA，进入 IPv6 NDRA 配置页面，如下图所示。如选择 NDRA 模式则接口作为主机经由能够发布 RA 报文的路由器获取地址。

图1-9 IPv6 NDRA 配置界面



1.1.6 以太网接口配置举例

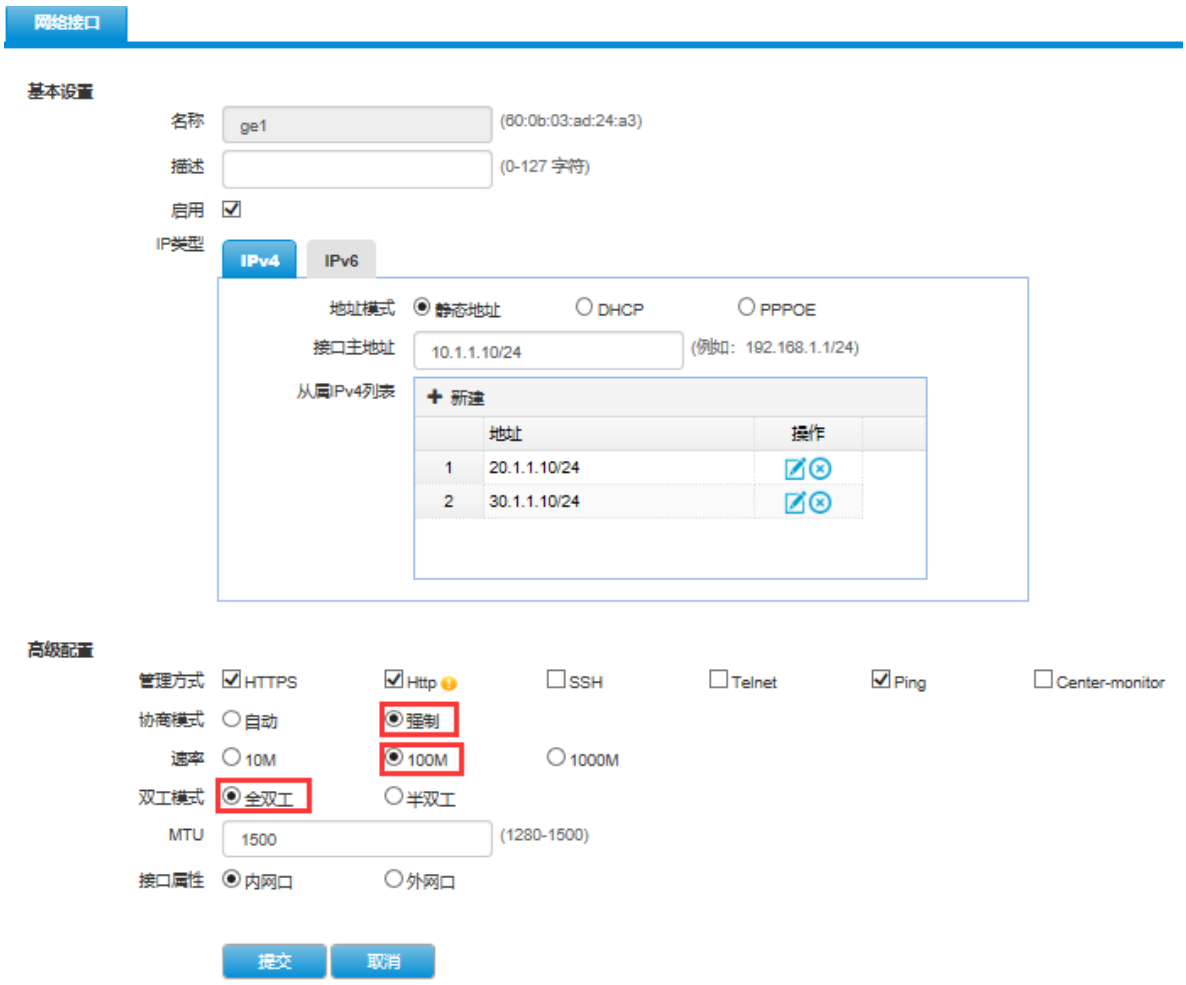
1. 组网需求

配置以太网接口 ge1 为百兆全双工模式，并给接口配置主 IP 地址 10.1.1.10/24 以及两个从 IP 地址 20.1.1.10/24 和 30.1.1.10/24。

2. 配置步骤

(1) 如图 1-10 所示，通过菜单“网络管理>接口配置>物理接口”打开以太网接口显示页面，点击 ge1 接口后的<编辑>图标，在弹出的页面中对 ge1 进行配置。

图1-10 ge1 接口配置页面



(2) 如图 1-11 所示，点击<提交>按钮后，可以在显示页面中看到我们对 ge1 的修改。

图1-11 以太网接口显示页面

1.2 VLAN接口配置

1.2.1 VLAN 概述

在一个物理局域网内，通过对端口的划分，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地通讯，而当分属不同群组的设备要进行通讯时，必须进行三层的路由转发；

通过这种方式，一个物理局域网就如同被划分为几个相互隔离的局域网，这些不同的群组就称为虚拟局域网（VLAN）。

VLAN 接口是一种三层模式下的虚拟接口，主要用于实现 VLAN 间的三层互通。它不作为物理实体存在于设备上。每个 VLAN 对应一个 VLAN 接口，该 VLAN 接口可以为本 VLAN 内端口收到的报文进行网络层转发操作。

VLAN 接口是虚端口，可以根据需要创建，同时也可以把不需要的 VLAN 接口删除。

1.2.2 VLAN 接口创建

如图 1-12 所示，通过菜单“网络配置 > 接口配置 > 子接口”使用该功能。点击网络子接口显示界面中的<新建>按钮，切换到子接口创建页面。

图1-12 VLAN 接口创建界面

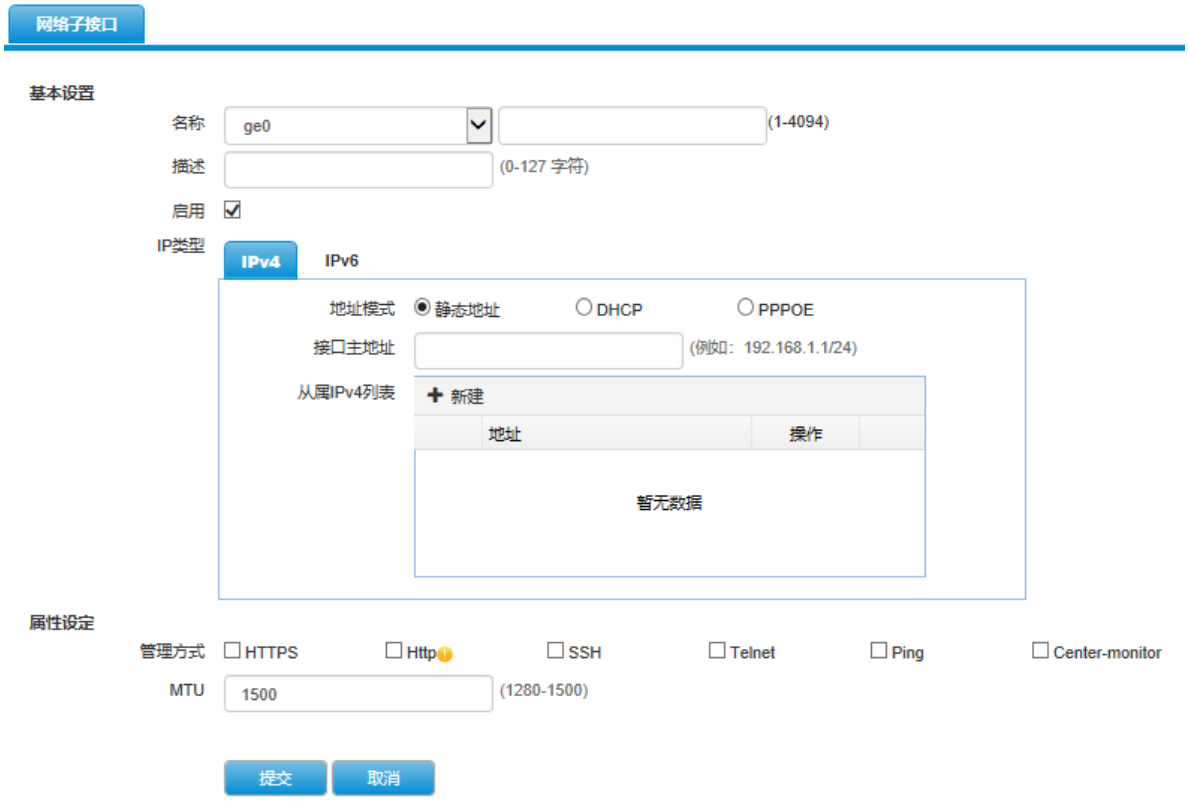


表1-9 配置说明

配置项	说明
名称	新建子接口的名称，物理接口+id，其中id可选为1~4094。
描述	接口描述。
启用	是否允许启用VLAN接口，缺省情况下为启用。
IP类型	IPv4地址和IPv6地址， 点击相应的标签，配置对应类型的IP地址。
地址模式	子接口的IPv4地址也可以通过以下三种方式获取：静态配置、DHCP、PPPoE方式，具体配

配置项	说明
	置可以参考物理端口配置。 子接口的IPv6地址也可以通过以下四种方式获取：静态配置、DHCP、PPPoE、NDRA方式，具体配置可以参考物理接口配置。
管理方式	配置端口是否允许HTTPS、HTTP、SSH、Telnet、PING等管理服务
MTU	接口发送报文的最大长度，缺省为1500，单位为字节。

1.2.3 VLAN 接口显示

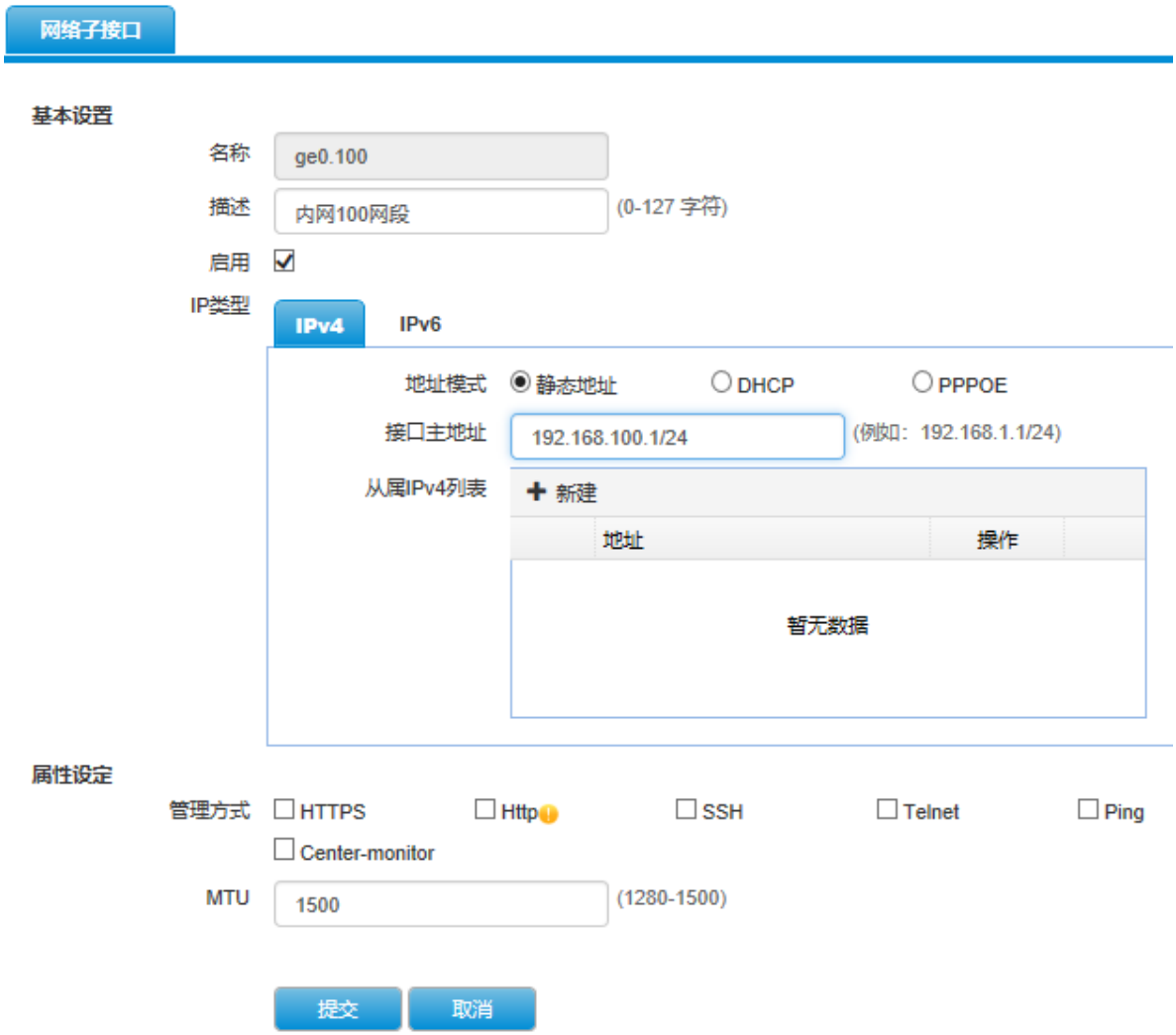
如图 1-13 所示，点击导航栏的“网络管理>接口配置>子接口”，点击子接口标签页，进入 VLAN 接口显示界面。

图1-13 VLAN 接口显示界面

1.2.4 VLAN 接口修改

如图 1-14 所示，通过菜单“网络配置 > 接口配置 > 子接口”使用该功能。点击网络子接口显示页面的编辑图标，切换到编辑页面。

图1-14 VLAN 接口编辑界面



1.2.5 VLAN 接口删除

通过菜单“网络配置 > 接口配置 > 子接口”使用该功能。点击网络子接口显示页面图 1-13 的删除图标，删除 VLAN 接口。

1.3 桥接口配置

1.3.1 桥接口概述

透明网桥使用方便，易于安装。当桥接入互连的局域网内，就能运行。它不会影响现存的局域网，原有的软硬件无须改变，也不要设置地址开关和加载路径选择表参数，对于用户来说，该网桥是透明的，即该网桥进入或离开整个网络，用户感觉不到。

1.3.2 桥接口创建

如图 1-15 所示，通过菜单“网络配置 > 接口配置 > 网桥接口”使用该功能。点击<新建>按钮，切换到网桥接口新建界面。

图1-15 桥接口新建界面

表1-10 配置说明

配置项	说明
名称	桥接口名称bvi+id，id可选为0~255。
描述	接口描述。
网桥可选接口	可加入桥接口的接口，包括没有子接口的物理接口和新建的子接口。
启用	是否允许启用桥接口，缺省情况下为启用。
IP类型	IPv4地址和IPv6地址， 点击相应的标签，配置对应类型的IP地址。
地址模式	网桥接口的IPv4地址也可以通过以下三种方式获取：静态配置、DHCP、PPPoE方式，具体配置可以参考物理端口配置； 网桥接口的IPv6地址也可以通过以下四种方式获取：静态配置、DHCP、PPPoE、NDRA方式，具体配置可以参考物理接口配置。
管理方式	配置端口是否允许HTTPS、HTTP、SSH、Telnet、PING等管理服务。

配置项	说明
MTU	接口发送报文的最大长度，缺省为1500，单位为字节。

1.3.3 桥接口显示

如图 1-16 所示，通过菜单“网络管理>接口>网桥接口”使用该功能。

图1-16 桥接口显示界面

1.3.4 桥接口修改

如图 1-17 所示，通过菜单“网络管理>接口>网桥接口”使用该功能。点击网桥接口显示页面的编辑图标，切换到编辑页面。

图1-17 网桥接口编辑界面

1.3.5 桥接口删除

通过菜单“网络配置 > 接口配置 > 网桥接口”使用该功能。点击网桥接口显示页面图 1-16 的删除图标，删除桥接口。

1.4 聚合接口配置

1.4.1 接口聚合概述

接口汇聚，就是通过配置软件的设置，将 2 个或多个物理端口组合在一起成为一条逻辑的路径从而增加在交换机和网络节点之间的带宽，将属于这几个端口的带宽合并，给端口提供一个几倍于独立端口的独享的高带宽。将多个物理链路捆绑在一起后，不但提升了整个网络的带宽，而且数据还可以同时经由被绑定的多个物理链路传输，具有链路冗余的作用，在网络出现故障或其它原因断开其中一条或多条链路时，剩下的链路还可以工作。

1.4.2 聚合接口创建

如图 1-18 所示，通过菜单“网络配置 > 接口配置 > 聚合接口”使用该功能。点击<新建>按钮，切换到聚合接口新建界面。

图1-18 聚合接口创建界面

表1-11 配置说明

配置项	说明
名称	聚合接口名称agg+id，id可选为0~255。
描述	接口描述。
接口列表	可加入聚合接口的接口。
启用	是否允许启用聚合接口，缺省情况下为启用。
IP类型	IPv4地址和IPv6地址， 点击相应的标签，配置对应类型的IP地址。
地址模式	聚合接口的IPv4地址也可以通过以下三种方式获取：静态配置、DHCP、PPPoE方式，具体配置可以参考物理端口配置； 聚合接口的IPv6地址也可以通过以下四种方式获取：静态配置、DHCP、PPPoE、NDRA方式，具体配置可以参考物理接口配置。
管理方式	配置端口是否允许HTTPS、HTTP、SSH、Telnet、PING等管理服务。

配置项	说明
MTU	接口发送报文的最大长度，缺省为1500，单位为字节。
负载分担	选择聚合口接口分流方式，按流条数分流或者按包分流。

1.4.3 聚合接口显示

如图 1-19 所示，通过菜单“网络管理>接口>聚合接口”使用该功能。

图1-19 聚合接口显示界面

1.4.4 聚合接口修改

如图 1-20 所示，通过菜单“网络配置 > 接口配置 > 聚合接口”使用该功能。点击图 1-19 聚合接口显示页面的编辑图标，切换到编辑页面。

图1-20 聚合接口编辑界面

1.4.5 聚合接口删除

通过菜单“网络配置 > 接口配置 > 聚合接口”使用该功能。点击图 1-19 聚合接口显示页面中的删除图标，删除聚合接口。

1.5 隧道接口配置

1.5.1 隧道接口概述

隧道接口作为设备的内部口，有 4 种模式：GRE 隧道接口、IPSEC 隧道接口、ipv6ip 隧道接口、sslvpn 隧道接口，这些隧道接口只能通过 CLI 创建，WEB 可以进行查看和编辑。

1.5.2 隧道接口创建

略

1.5.3 隧道接口显示

如图 1-21 所示，通过菜单“网络管理>接口配置>隧道接口”使用该功能。

图1-21 隧道接口显示界面

1.5.4 隧道接口修改

如图 1-22 所示，通过菜单“网络配置 > 接口配置 > 隧道接口”使用该功能。点击图 1-21 隧道接口显示页面的编辑图标，切换到编辑页面。

图1-22 隧道接口编辑界面

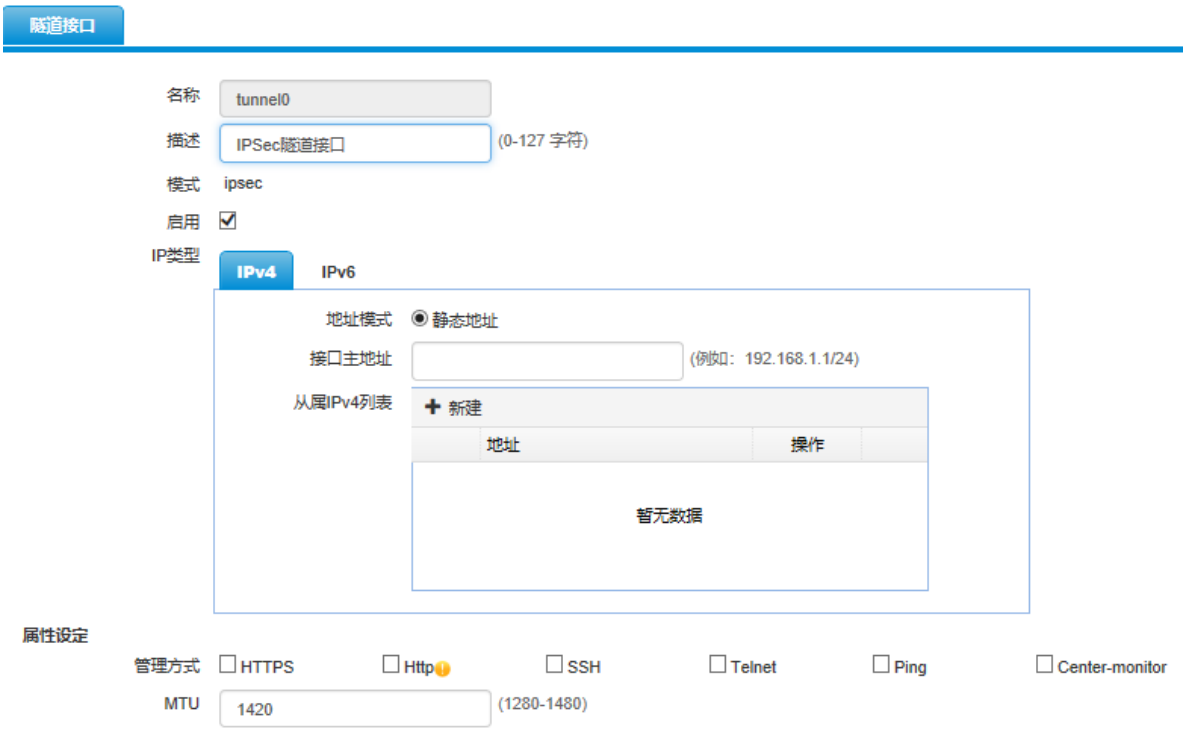


表1-12 配置说明

配置项	说明
名称	隧道接口名称+id，id可选为0~1023
描述	接口描述
模式	隧道接口模式
启用	是否允许启用隧道接口，缺省情况下为启用
IP类型	IPv4地址和IPv6地址 点击相应的标签，配置对应类型的IP地址
地址模式	隧道接口的IPv4地址或IPV6地址只能通过静态配置

配置项	说明
管理方式	配置端口是否允许HTTPS、HTTP、SSH、Telnet、PING等管理服务
MTU	接口发送报文的最大长度，IPSEC隧道缺省为1420，GRE隧道缺省为1476，Ipv6隧道缺省为1480，单位为字节

1.6 无线接口配置

1.6.1 无线接口概述

无线接口作为设备的外置接口，支持通过插 4G 网卡的方式，让设备接入网络，为上网需求量较少或者没有条件架设有线设施的用户解决访问网络的需求。

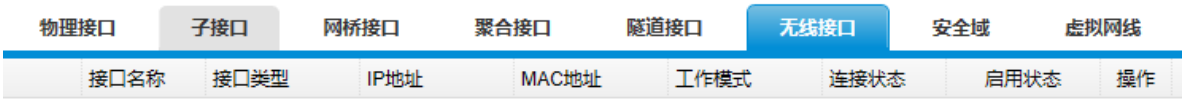
1.6.2 无线接口创建

设备 USB 口插上 4G 网卡后自动创建，无需人为创建。

1.6.3 无线接口显示

如图 1-23 所示，通过菜单“网络管理>接口配置>无线接口”使用该功能。

图1-23 无线接口显示界面



1.6.4 无线接口修改

如图 1-24 所示，通过菜单“网络配置 > 接口配置 > 无线接口”使用该功能。点击图 1-23 无线接口显示页面的编辑图标，切换到编辑页面。

图1-24 无线接口编辑界面

表1-13 配置说明

配置项	说明
厂商	4G网卡所属厂商
接口名称	接口名称，自动生成
MAC地址	4G网卡MAC地址
IP地址	4G接口IP地址，自动获取
地址类型	DHCP获取，无法修改
网关	下一跳地址，自动获取
DNS	DNS地址，自动获取
启用	是否允许启用无线接口，缺省情况下为启用
更新网关	自动生成默认路由

配置项	说明
更新DNS	自动获取DNS
权重	路由权重
MTU	接口发送报文的最大长度，缺省为1500，单位为字节

1.7 配置安全域

1.7.1 背景信息

安全区域（Security Zone）简称区域（Zone），是设备所引入的一个安全概念，安全策略可以基于安全区域实施。

设备默认无安全域，也没有默认的安全域间的访问策略，需要手动配置。将接口加入安全域后，可以更加方便地在策略里进行引用。

1.7.2 安全域创建

如图 1-22 所示，通过菜单“网络管理>接口配置>安全域”使用该功能。单击“新建”进入安全域创建界面。

图1-25 配置安全域界面

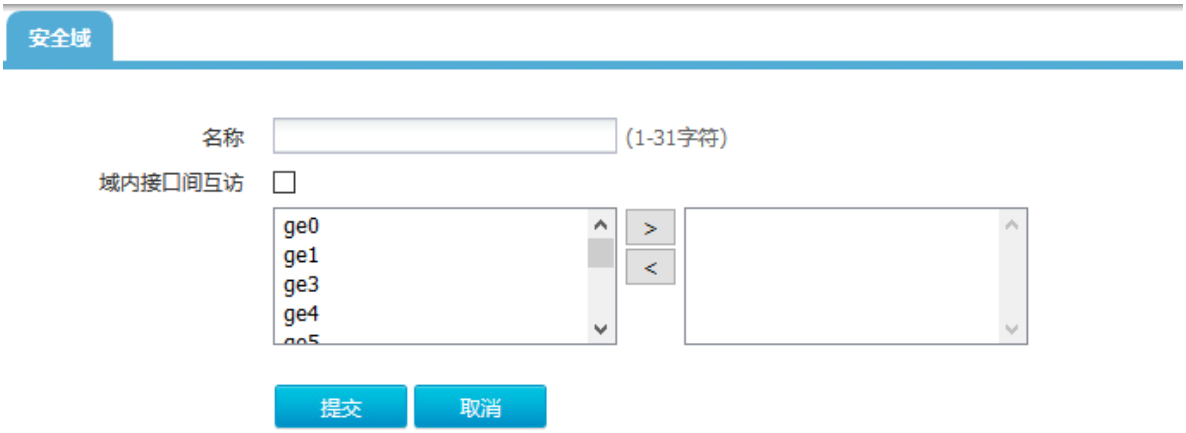


表1-14 配置安全域的参数

参数	说明
名称	安全域的名称。安全区域名称一旦设定，不允许更改。
域内接口间访问	控制域内接口能否互访，默认不允许互访。
安全域可选接口	左侧为可选加入安全域的接口。
安全域已选接口	右侧为已选的安全域接口。

1.7.3 安全域显示

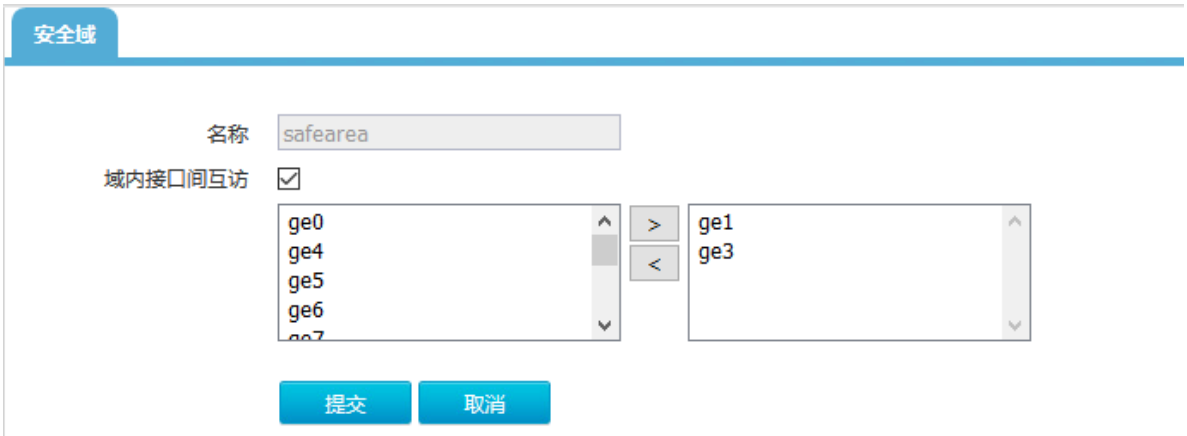
如图 1-23 所示，通过菜单“网络管理>接口配置>安全域”使用该功能。

图1-26 安全域的显示

1.7.4 安全域修改

如图 1-24 所示，通过菜单“网络管理>接口配置>安全域”使用该功能。单击对应安全域中操作栏里的“修改”按钮进入修改界面。

图1-27 安全域的修改



1.7.5 安全域删除

通过菜单“网络管理>接口>安全域”使用该功能。单击对应安全域中操作栏里的“删除”按钮即可删除对应的安全域。

1.8 配置虚拟网线

1.8.1 背景信息

信息与网络安全被越来越多的客户认知，越来越多的客户在实际网络拓扑中部署安全设备，传统的部署方式需要对客户的网络拓扑比较了解，甚至需要更改网络设备的配置，虚拟网线方式提供一种无感知方式，不需要客户对原有的网络拓扑做任何更改，虽然桥接方式也可以满足一部分要求，但虚拟网线免去了 MAC 学习和二层交换，避免了因 MAC 错乱导致的问题，同时虚拟线相比于传统的

桥接方式效率更高。此外虚拟网线还附加了端口联动和 vlan 过滤功能以此来满足透明接入的实际需求。

1.8.2 虚拟网线创建

如图 1-28 所示，通过菜单“网络管理>接口>虚拟网线”使用该功能。单击“新建”进入虚拟网线创建界面。

图1-28 配置虚拟网线界面

表1-15 配置虚拟网线的参数

参数	说明
名称	虚拟网线的名称。虚拟网线名称一旦设定，不允许更改。
描述	虚拟网线描述。
接口1	加入虚拟网线的物理接口1。
接口2	加入虚拟网线的物理接口2。
vlan允许范围	配置虚拟网线允许的vlan 范围，只允许配置的vlan范围通过。
端口联动	配置虚拟网线端口联动，虚拟网线中的一个接口down，另一个接口也会down。

1.8.3 虚拟网线显示

如图 1-29 所示，通过菜单“网络管理>接口配置>虚拟网线”使用该功能。

图1-29 虚拟网线的显示

1.8.4 虚拟网线修改

如图 1-30 所示，通过菜单“网络管理>接口配置>虚拟网线”使用该功能。单击对应虚拟网线中操作栏里的“修改”按钮进入修改界面。

图1-30 虚拟网线的修改

1.8.5 虚拟网线删除

通过菜单“网络管理>接口配置>虚拟网线”使用该功能。单击对应虚拟网线中操作栏里的“删除”按钮即可删除对应的虚拟网线。

1.9 VLAN接口，桥接口，聚合接口创建及交互举例

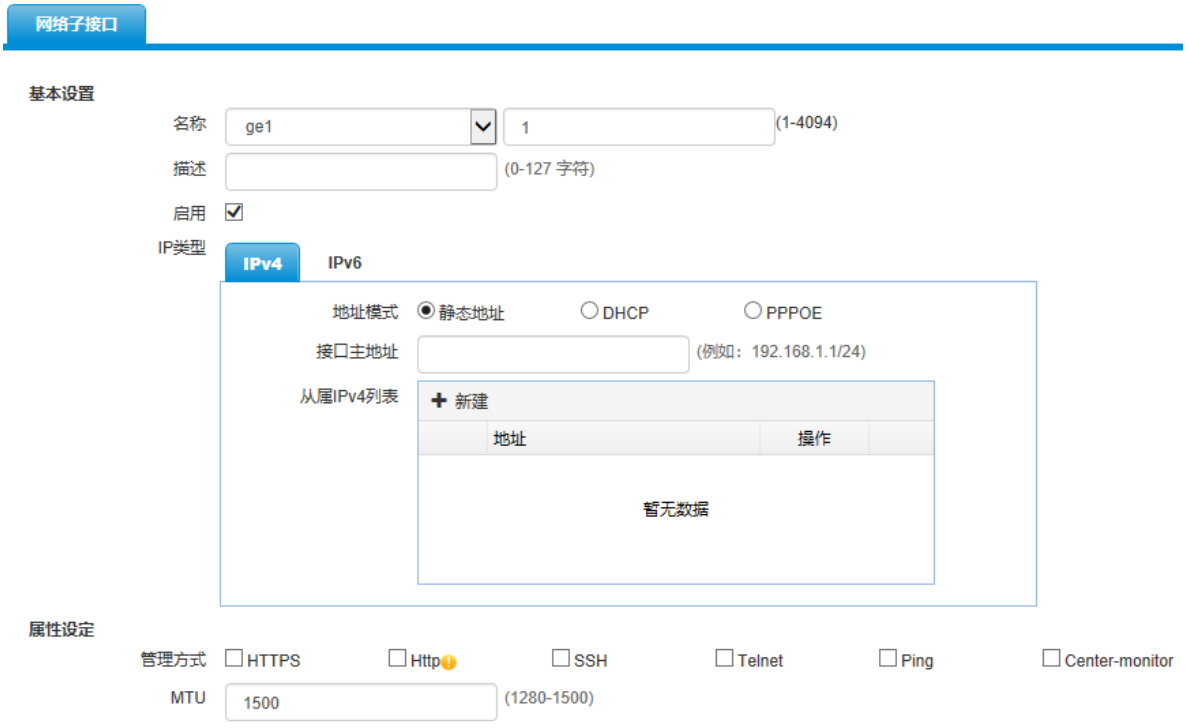
1. 组网需求

创建 VLAN 接口 ge1.1，桥接口 bvi0 以及聚合接口 agg0，将 ge2 接口加入 agg0 接口，将 agg0 以及 ge1.1 加入桥接口 bvi0，并且给桥接口配置 IP 地址 40.1.1.10/24。

2. 配置步骤

(1) 如图 1-31 所示，通过菜单“网络管理>接口配置>子接口”打开子接口显示页面，点击<新建>按钮，在弹出的页面中进行配置。

图1-31 VLAN 接口 ge1.1 创建页面

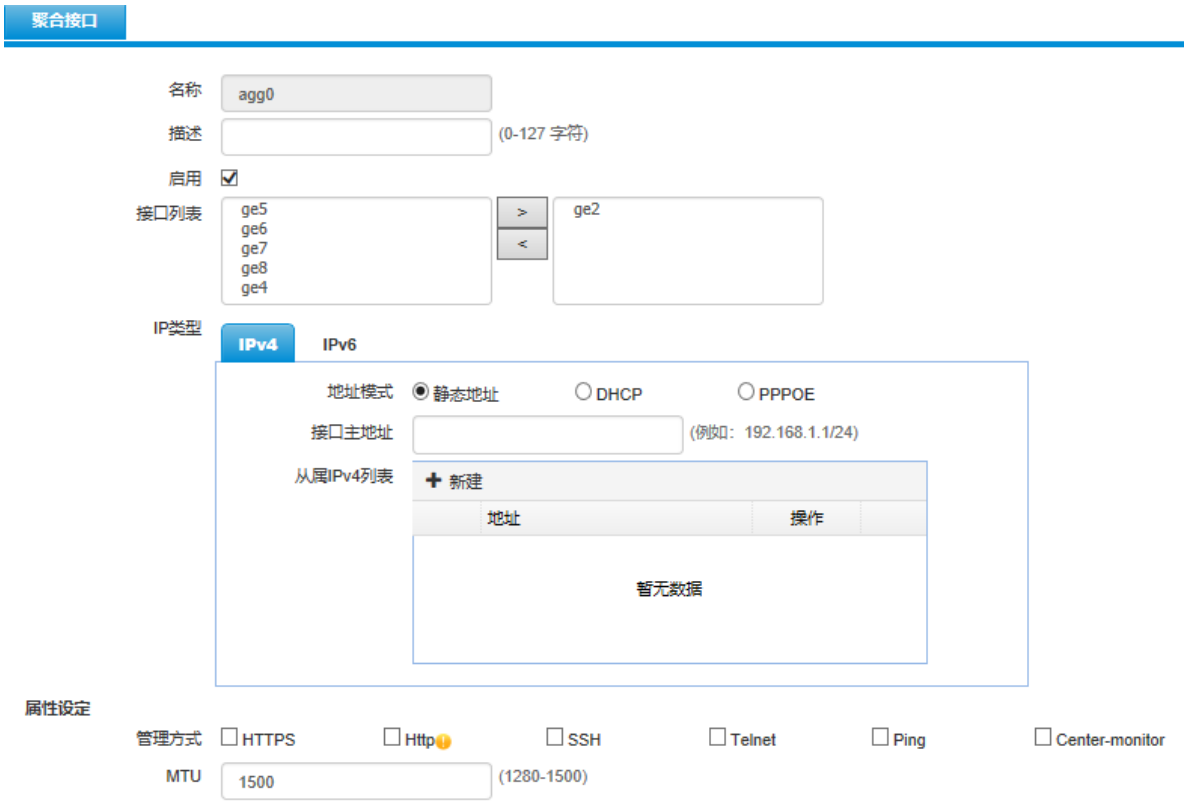


(2) 如图 1-32 所示，点击<提交>按钮，可以看到显示页面中的 ge1.1 接口。

图1-32 子接口显示页面

(3) 如图 1-33 所示，创建并配置 agg0：过菜单“网络配置 > 接口配置 > 聚合接口”打开聚合接口显示页面，点击<新建>按钮，在弹出的页面中进行配置，agg0 接口包含 ge2 以太网接口，其它使用缺省配置。

图1-33 agg0 配置页面



(4) 如图 1-34 所示，点击<提交>按钮后，可以在聚合接口的显示页面中看到我们创建的 agg0 接口。

图1-34 聚合接口显示页面

(5) 如图 1-35 所示，创建并配置 bvi0：过菜单“网络管理>接口配置>网桥接口”打开网桥接口显示页面，点击<新建>按钮，在弹出的页面中进行配置，bvi0 接口包含我们在前面步骤中创建的 VLAN 接口 ge1.1 和聚合接口 agg0，并配置其 IP 地址为 40.1.1.10/24，其它使用缺省配置。

图1-35 bvi0 创建页面

(6) 如图 1-36 所示，点击<提交>按钮后，可以在网桥接口显示页面中，看到我们创建的接口以及加入该网桥接口的接口列表。

图1-36 网桥接口显示页面

1.10 配置IPv6隧道接口

1.10.1 隧道技术概述

隧道技术是一种通过互联网络基础设施在网络之间传递数据的方式。使用隧道传递的数据可以是不同协议的数据帧或包，隧道协议将这些其它协议的数据帧或包重新封装在新的包头中发送，被封装

的数据包在隧道的两个端点之间通过公共互联网络进行路由，一旦到达网络终点，数据将被解包并转发到最终目的地。整个传递过程中，被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。

简言之，隧道技术是指包括数据封装，传输和解包在内的全过程。

本设备支持两种封装模式的隧道接口：IPsec 封装和 IPv6 封装。本章重点讲解 IPv6 封装模式的隧道接口，关于 IPsec 封装的详细介绍，请参见 1.11 。

1.10.2 IPv6 隧道接口创建

通过菜单“网络配置>基础网络>IPv6 网络>IPv6 隧道”使用该功能。如图 1-37 所示，点击<新建>按钮，切换到 IPv6 隧道新建界面。

图1-37 IPv6 隧道接口新建界面

表1-16 配置说明

配置项	说明
名称	创建时会根据当前tunnel id的使用情况，给一个推荐的可用的tunnel id
隧道模式	一共三种模式：手工隧道（manual），isatap和6to4，点击不同的单选按钮，出现不同的配置选项 上面是manual模式的配置选项
隧道源	隧道的源地址模式： 选择地址模式时，使用源地址作为隧道源 选择接口模式时，选择设备上的接口作为隧道源
隧道目的	隧道接口的目的地址，只有manual模式时需要填写

注意

每个接口都能分别配置不同的封装模式，但每次只能配置一种方式，且在接口创建时就指定，不能修改。

如图 1-38、图 1-39 所示，下面是 isatap 和 6to4 的配置选项。相比 manual，isatap 和 6to4 少了隧道目的地址的配置。

图1-38 隧道接口 isatap 模式

图1-39 隧道接口 6to4 模式

1.10.3 IPv6 隧道接口修改

如图 1-40 所示，通过菜单“网络配置 > 基础网络 > IPv6 网络 > IPv6 隧道”使用该功能。

点击选定接口的编辑按钮，切换到编辑界面。

图1-40 IPv6 隧道接口编辑界面

说明

隧道接口的名称、隧道模式都不能修改，只能在创建时指定。

1.10.4 IPv6 隧道接口删除

如图 1-41 所示，通过菜单“网络配置>基础网络>IPv6 网络>IPv6 隧道”使用该功能。

点击删除按钮，删除选定的接口。

图1-41 IPv6 隧道接口删除界面

1.10.5 IPv6 隧道接口属性配置

如图 1-42 所示，通过菜单“网络配置 > 接口配置 > 隧道接口”使用该功能。

点击选定接口的<编辑>按钮，切换到编辑界面。

图1-42 隧道接口属性编辑界面

注意

在该页内，只能对接口相关的属性进行编辑，如 IPv4/IPv6 地址，MTU 等。

1.10.6 IPv6 隧道接口配置举例

1. 组网需求

创建一个 IPv6 手工隧道接口，并设置源接口为 ge4，目的地址为 100.1.1.10，且给隧道接口配置 IP 地址为 50.1.1.10/24。

2. 配置步骤

(1) 如图 1-43 所示，通过菜单“网络配置>基础网络>IPv6 网络>IPv6 隧道”打开显示页面，点击<新建>按钮，配置隧道接口的名称，隧道模式，隧道源，源接口及隧道目的。

图1-43 隧道接口新建页面

(2) 如图 1-44 所示，点击<提交>按钮后，可以在显示页面中看到我们配置的隧道接口。

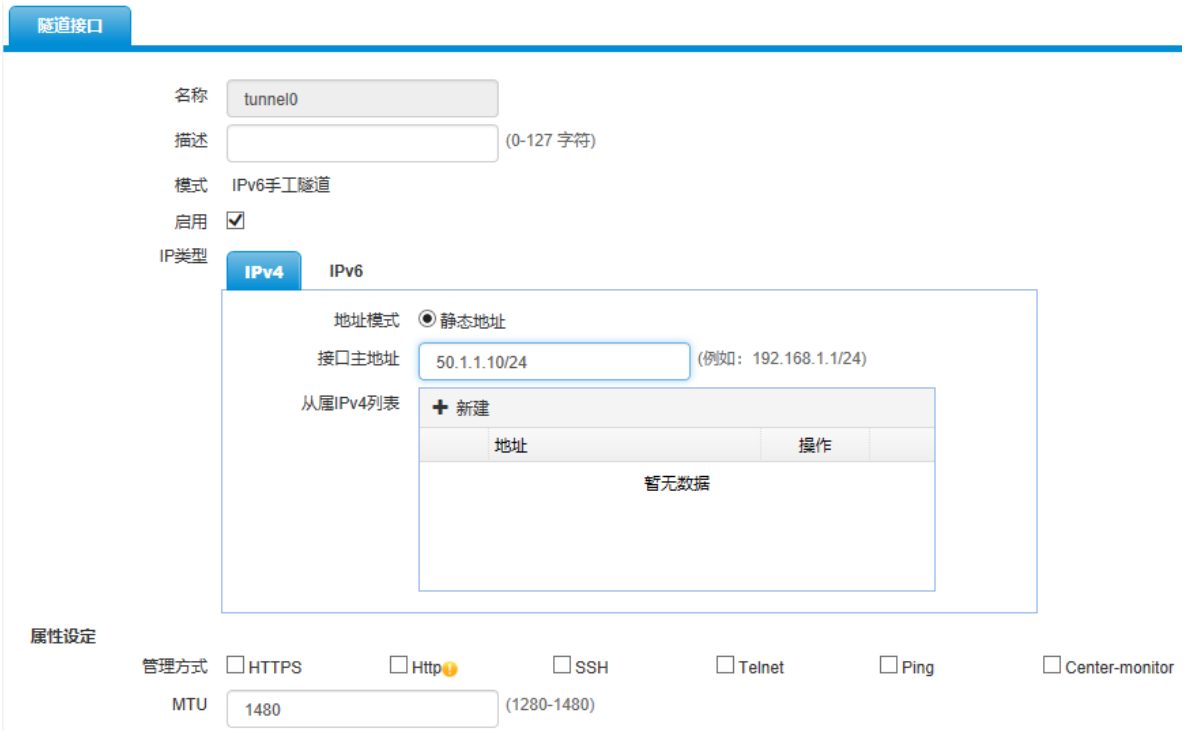
图1-44 隧道接口显示

(3) 如图 1-45 所示，给隧道接口配置 IP 地址，需要转移到接口页面中，通过菜单“网络管理>接口配置>隧道接口”打开显示页面，点击 tunnel0 接口对应的<编辑>按钮，打开编辑页面。

图1-45 tunnel0 接口属性显示页面

(4) 如图 1-46 所示，给 tunnel0 接口配置 IP 地址，点击<提交>按钮提交。

图1-46 tunnel 接口属性配置页面



1.11 配置IPsec隧道接口

1.11.1 IPsec 隧道接口创建

如图 1-47 所示，通过菜单“网络配置>VPN>IPsec-VPN>IPsec 第三方对接>IPsec 隧道接口”使用该功能。

点击<新建>按钮，切换到 IPsec 隧道新建界面。

图1-47 IPsec 隧道接口新建界面

表1-17 配置说明

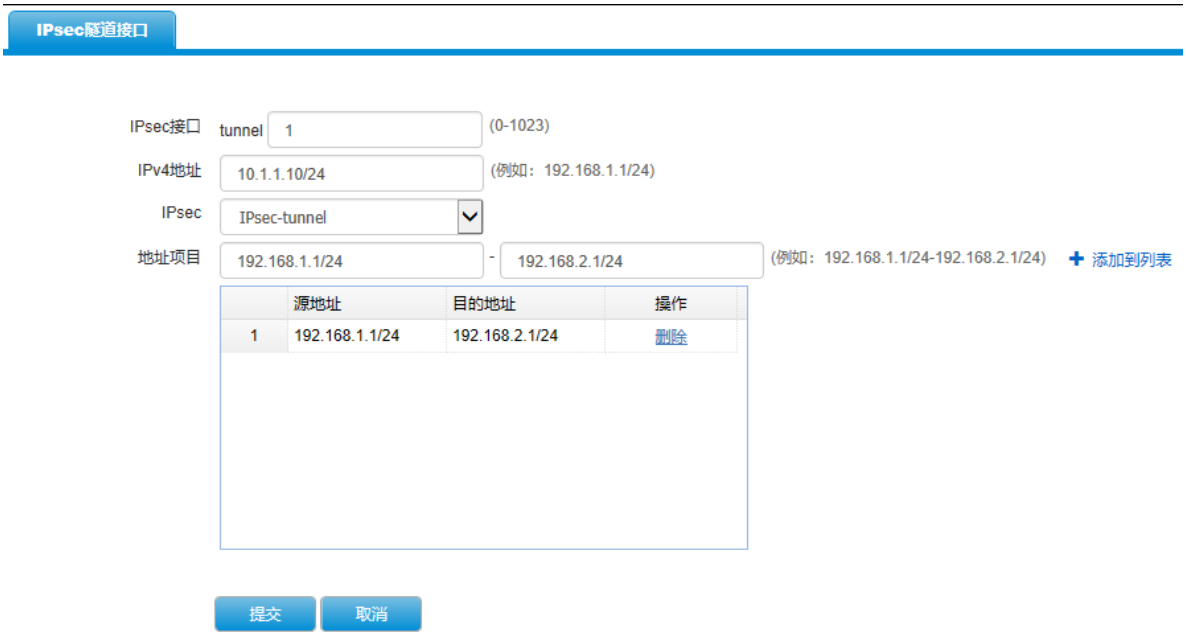
配置项	说明
IPsec接口	创建时会根据当前tunnel id的使用情况，给一个推荐的可用的tunnel id
IPv4地址	隧道接口的IP地址
IPsec	设备上的IPsec隧道
地址项目	tunnel口绑定IPsec隧道的同时，可以选择性的配置一个保护网段 该保护网段即为IPsec的感兴趣流，用于第二阶段SA的协商 保护网段（感兴趣流）以地址对象的形式进行配置

1.11.2 IPsec 隧道接口修改

如图 1-48 所示，通过菜单“网络配置>VPN>IPsec-VPN> IPsec 第三方对接>IPsec 隧道接口”使用该功能。

点击选定接口的<编辑>按钮，切换到编辑界面。

图1-48 IPsec 隧道接口编辑界面



1.11.3 IPsec 隧道接口删除

如图 1-49 所示，通过菜单“网络配置>VPN>IPsec-VPN> IPsec 第三方对接>IPsec 隧道接口”使用该功能。

点击<删除>按钮，删除选定的接口。

图1-49 IPsec 隧道接口删除界面

1.11.4 IPsec 隧道接口属性配置

如图 1-50 所示，通过菜单“网络管理>接口配置>隧道接口”使用该功能。

点击选定接口的<编辑>按钮，切换到编辑界面。

图1-50 IPsec 隧道接口属性配置

1.11.5 IPec 隧道接口配置举例

1. 组网需求

创建一个 IPsec 隧道接口。由于 IPsec 隧道接口的特殊性，需要先创建 IKE，然后建 IPsec，然后再创建 IPsec tunnel。

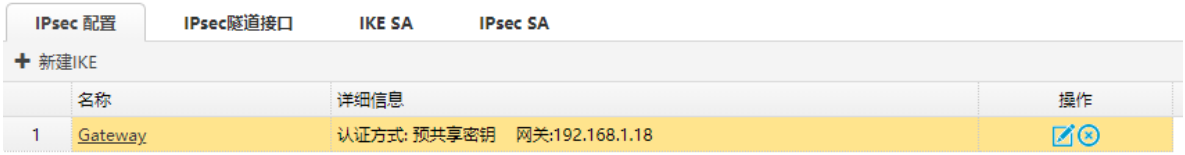
2. 组网图

(1) 如图 1-51 所示，通过菜单“网络配置>VPN>IPsec-VPN>IPsec 第三方对接>IPsec 配置”打开 IKE 列表，点击“新建 IKE”，创建一个名为 Gateway 的 IKE。

图1-51 IKE 新建页面

(2) 如图 1-52 所示，点击<提交>按钮后，可以在显示页面看到我们创建的这个 IKE。

图1-52 IPsec 显示页面



(3) 如图 1-53 所示，点击图 1-52 IPsec 显示页面的<新建 Ipsec>按钮，在弹出的配置页面中创建 IPsec。

图1-53 IPsec 新建页面

(4) 如图 1-54 所示，点击<提交>按钮后，可以在显示页面看到我们创建的这个 IPsec_tunnel。

图1-54 IPsec 显示页面

(5) 如图 1-55 所示，通过菜单“网络配置>VPN>IPsec-VPN>IPsec 第三方对接>IPsec 隧道接口”打开 IPsec 隧道显示页面，点击<新建>按钮，切换到 IPsec 隧道新建界面。

图1-55 IPsec 隧道新建界面

(6) 如图 1-56 所示，点击<提交>按钮后，可以在显示页面看到我们创建的 tunnel 接口。

图1-56 IPsec 隧道接口显示

(7) 其它接口属性，如从属 IP 地址，接口管理方式，MTU 等，需要切换到接口属性配置页面中配置。通过菜单“网络管理>接口配置>隧道接口”实现，同 IPv6 隧道接口的属性配置。

目 录

1 静态路由 ····· 1-1
1.1 概述 ····· 1-1
1.2 静态路由表 ····· 1-1
1.3 静态路由配置 ····· 1-2
1.4 配置举例 ····· 1-3
1.4.1 静态路由配置举例 ····· 1-3

1 静态路由

1.1 概述

静态路由是在设备中设置的固定的路由。除非网络管理员干预，否则静态路由不会发生变化。由于静态路由不能对网络的改变作出反映，一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。在所有的路由中，静态路由优先级最高。当动态路由与静态路由发生冲突时，以静态路由为准。

1.2 静态路由表

通过菜单“网络配置 > 路由管理 > 静态路由”，进入如图 1-1 所示页面。在该页面上，可以查看已经配置的静态路由信息。这些信息的详细说明如表 1-1 所示。

图1-1 静态路由表

表1-1 静态路由表的显示信息

标题项	说明
目的地址	静态路由的目的IP地址
掩码	静态路由的网络掩码
下一跳	静态路由的下一跳的IP地址
出接口	静态路由的出接口，如果是null0，表示目的地址不可达
权重	静态路由的权重
距离	静态路由的管理距离
地址探测	和静态路由联动的地址探测，如果已经配置和探测联动，点击地址探测名称可以修改和路由联动的地址探测
状态	表示已经生效，表示未生效
操作	可以执行删除操作

说明

- 权重：在多下一跳负载均衡时，当距离值相同，根据源地址哈希值按照权重比值分摊流量。
- 距离：路由类型的优先级，该值越小，优先级越高。

1.3 静态路由配置

通过点击图 1-1 中的“新建”，进入如图 1-2 所示页面。各配置项含义如表 1-2 所示。

图1-2 静态路由配置页面

表1-2 静态路由配置项含义

标题项	说明
启用	静态路由启用或禁用开关，勾选表示启用，不勾选表示禁用。
目的网段	设置静态路由的目的网段
子网掩码	设置静态路由的网络掩码，可以输入掩码长度或者点分十进制格式的掩码
下一跳	设置静态路由的下一跳的IP地址
出接口	设置静态路由的出接口 下一跳和出接口只能二选一
权重	设置静态路由的权重，范围是1到255

标题项	说明
距离	设置静态路由的管理距离，范围是是1到255
地址探测	设置路由和地址探测联动

说明

- 权重：在多下一跳负载均衡时，权重越大，命中的概率就越大。
- 距离：路由类型的优先级，该值越小，优先级越高。

1.4 配置举例

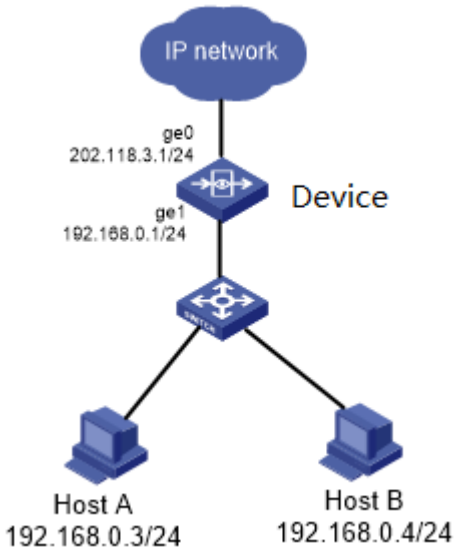
1.4.1 静态路由配置举例

1. 组网需求

各设备接口及主机的 IP 地址和掩码如图 1-3 所示。要求采用静态路由的默认路由，把每个没有对应路由的报文转发到公网地址 202.118.3.2。

2. 组网图

图1-3 静态路由配置案例组网图



3. 配置步骤

(1) 按照组网图组网。

(2) 通过菜单“网络配置 > 路由管理> 静态路由表”，点击<新建>，按照如图 1-4 所示配置默认路由。

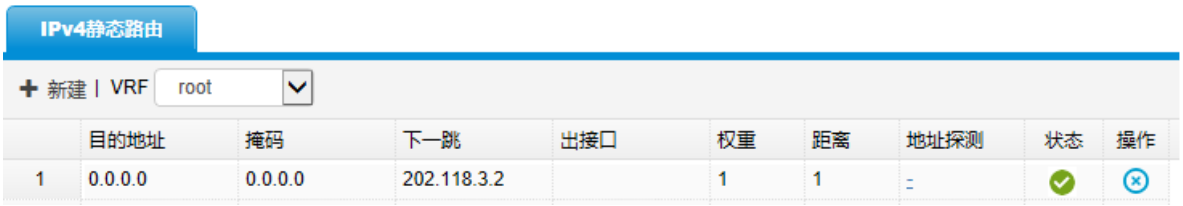
图1-4 静态路由配置

点击<提交>按钮，提交配置。

4. 验证配置

查看静态路由表，验证是否生效，如图 1-5 所示。

图1-5 验证配置



目 录

1 RIP ····· 1-1
1.1 RIP 概述 ····· 1-1
1.1.1 RIP 的工作机制 ····· 1-1
1.1.2 RIP 的版本 ····· 1-2
1.1.3 协议规范 ····· 1-2
1.2 全局设定 ····· 1-3
1.3 RIP 网络配置 ····· 1-4
1.4 RIPKeychain 配置 ····· 1-4
1.5 RIP 接口配置 ····· 1-5
1.6 配置举例 ····· 1-7
1.6.1 RIP 配置举例 ····· 1-7

1 RIP

1.1 RIP概述

本节介绍配置 RIP 所需要理解的知识，具体包括：

- RIP 的工作机制
- RIP 的版本
- 协议规范

RIP（Routing Information Protocol，路由信息协议）是一种较为简单的内部网关协议（Interior Gateway Protocol，IGP），主要用于规模较小的网络中，比如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用 RIP。由于 RIP 的实现较为简单，在配置和维护管理方面也远比 OSPF 和 IS-IS 容易，因此在实际组网中仍有广泛的应用。

1.1.1 RIP 的工作机制

1. RIP 的基本概念

RIP 协议是基于 D-V 算法（又称为 Bellman-Ford 算法）的内部动态路由协议，简称 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，是最广泛使用的 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 协议使用跳数来衡量到达信宿机的距离，并称为路由权， 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路的形成，并且使用触发更新和路由超时机制确保路由的正确性。

2. RIP 的启动和运行过程

RIP 启动和运行的整个过程可描述如下：

- 路由器启动 RIP 后，便会向相邻的路由器发送请求报文（Request message），相邻的 RIP 路由器收到请求报文后，响应该请求，回送包含本地路由表信息的响应报文（Response message）。
- 路由器收到响应报文后，修改本地路由表，同时向相邻路由器发送触发修改报文，广播路由修改信息。相邻路由器收到触发修改报文后，又向其各自的相邻路由器发送触发修改报文。在一连串的触发修改广播后，各路由器都能得到并保持最新的路由信息。
- RIP 采用老化机制对超时的路由进行老化处理，以保证路由的实时性和有效性。因此，RIP 每隔一定时间周期性的向邻居路由器发布本地的路由表，相邻路由器在收到报文后，对其本地路由进行更新。所有 RIP 路由器都会重复此过程。

3. 防止路由循环

RIP 是一种基于 D-V 算法的路由协议，由于它向邻居通告的是自己的路由表，存在路由循环的可能性。

RIP 通过以下机制来避免路由环路的产生：

- 水平分割（Split Horizon）：RIP 从某个接口学到的路由，不会从该接口再发回给邻居路由器。这样不但减少了带宽消耗，还可以防止路由循环。
- 毒性逆转（Poison Reverse）：RIP 从某个接口学到路由后，将该路由的开销设置为 16（不可达），并从原接口发回邻居路由器。利用这种方式，可以清除对方路由表中的无用信息。

1.1.2 RIP 的版本

RIP 有两个版本：RIP-1 和 RIP-2。

RIP-1 是有类别路由协议（Classful Routing Protocol），它只支持以广播方式发布协议报文。RIP-1 的协议报文中没有携带掩码信息，它只能识别 A、B、C 类这样的自然网段的路由，因此 RIP-1 无法支持路由聚合，也不支持不连续子网（Discontiguous Subnet）。

RIP-2 是一种无分类路由协议（Classless Routing Protocol），与 RIP-1 相比，它有以下优势：

- 支持外部路由标记（Route Tag），可以在路由策略中根据 Tag 对路由进行灵活的控制。
- 报文中携带掩码信息，支持路由聚合和 CIDR（Classless Inter-Domain Routing）。
- 支持指定下一跳，在广播网上可以选择到最优下一跳地址。
- 支持组播路由发送更新报文，减少资源消耗。
- 支持对协议报文进行验证，并提供明文验证和 MD5 验证两种方式，增强安全性。

说明

RIP-2 有两种报文传送方式：广播方式和组播方式，缺省将采用组播方式发送报文，使用的组播地址为 224.0.0.9。当接口运行 RIP-2 广播方式时，也可接收 RIP-1 的报文。

1.1.3 协议规范

与 RIP 相关的协议规范有：

- RFC1058：Routing Information Protocol
- RFC1723：RIP Version 2 - Carrying Additional Information
- RFC1721：RIP Version 2 Protocol Analysis
- RFC1722：RIP Version 2 Protocol Applicability Statement
- RFC1724：RIP Version 2 MIB Extension
- RFC2082：RIP-2 MD5 Authentication
- RFC2091：Triggered Extensions to RIP to Support Demand CircuitsRIP

1.2 全局设定

通过菜单“网络配置 > 路由管理 > RIP 信息”，进入如图 1-1 所示页面。在该页面上，可以配置 RIP 协议收发报文的版本、RIP 定时器及路由重发布信息。这些信息的详细说明如表 1-1 所示。

图1-1 RIP 全局设置

表1-1 RIP 设定页面各配置项说明

标题项	说明
启用	RIP路由的启禁用，勾选启用该路由，不勾选则不启用。
RIP版本	设置要使用的RIP版本。
向外发布缺省路由	设置是否向外发布缺省路由。
更新	设置RIP更新定时器，缺省情况下为30s。
超时	设置RIP超时时间，缺省情况下为180s。
失效	设置RIP失效时间，缺省情况下为120s。
直连路由	设置是否重发布直连路由，并设置直连路由的跳数。
静态路由	设置是否重发布静态路由，并设置静态路由的跳数。

标题项	说明
OSPF跳数	设置是否重发布OSPF路由，并设置OSPF路由的跳数

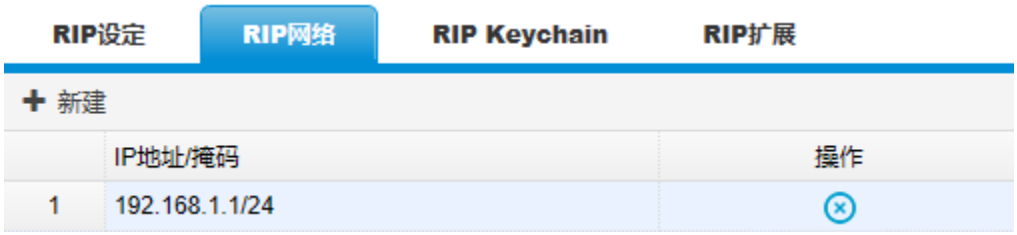
说明

RIP 会根据定时更新时间周期向外发布整个路由表，如果超时时间到达时还没有收到某条路由的更新，就把这条路由从内核路由表中删除，并把 metric 置为 16 向外发布，并设置失效定时器；失效时间到达时，把这条路由在 RIP 路由表中删除。

1.3 RIP网络配置

(1) 通过点击图 1-1 中的“RIP 网络”，进入如图 1-2 所示页面。该页显示了已经配置的 RIP 网络，在该页也可以删除已经配置的 RIP 网络。

图1-2 RIP 网络显示界面



(2) 点击图 1-2 中的<新建>按钮，进入如图 1-3 所示页面，在该页填入要发布的 RIP 网络，点击<提交>按钮，完成 RIP 网络的配置。

图1-3 RIP 网络配置界面

1.4 RIPKeychain配置

选择“网络配置 > 路由管理 > RIP 信息 > RIP Keychain”，单击“新建”按钮进入 RIP Keychain 配置页面，如图 1-4 所示。

图1-4 RIPKeychain 配置界面

表1-2 RIPKeychain 配置参数

参数	说明
名称	Keychain名称，在本地生效。
Key值	Key-ID值，在双方认证时需要保持一致。
密码	Keychain密码，在双方认证时需要保持一致。

1.5 RIP接口配置

(1) 点击图 1-1 中的“RIP 扩展”，进入所示图 1-5 页面。该页面显示了已经配置的接口信息，具体信息说明如表 1-3 所示。

图1-5 RIP 扩展

表1-3 RIP 扩展各项含义

标题项	说明
接口名称	已经配置的接口名称
发送版本	该接口可发送RIP的版本
接收版本	该接口可接收RIP的版本
认证算法	接口所使用的加密方式，有明文、密文及不认证
操作	点击可以对该配置进行修改，点击可以删除该配置

(2) 点击图 1-5 中的<新建>按钮，进入如图 1-6 所示页面。该页面可以配置接口相关的 RIP 信息，具体信息说明如表 1-4 所示。

图1-6 RIP 接口配置

表1-4 RIP 接口各项配置含义

标题项	说明
接口	选择要配置接口
发送版本	设置该接口可发送RIP的版本
接收版本	设置该接口可接收RIP的版本
认证方式	选择认证方式：无、明文、密文，不进行认证时一般选择无。
认证标记	选择认证标记：Keychain、密码，进行认证时双方验证的参数。

1.6 配置举例

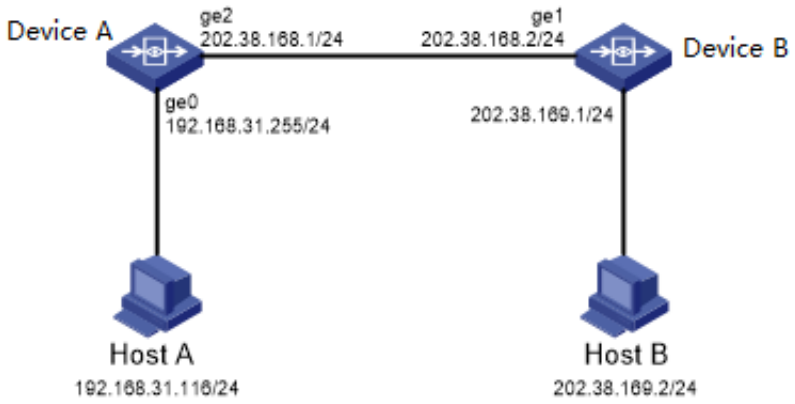
1.6.1 RIP 配置举例

1. 组网需求

按照图 1-7 所示，配置接口 IP 地址，要求设备 A 在 ge0 和 ge2 接口上启用了 RIP，设备 B 在接口 ge0 和 ge1 上启用了 RIP，两个设备的互连的接口收发报文的版本都设置为 2。

2. 组网图

图1-7 RIP 配置案例组网图



3. 配置步骤

(1) 按照组网图组网。

(2) 配置设备 A。

- 通过菜单“网络配置 > 路由管理 > RIP 信息 > RIP 设定”，进入 RIP 全局配置，如图 1-8 所示，点击<提交>按钮。

图1-8 RIP 全局配置

- 点击图 1-9 中的“RIP 网络”，进入如图 1-2 所示页面，点击新建，进入如图 1-9 所示页面，分别配置网络 202.38.168.1/24 和 192.168.31.225/24，并点击<提交>按钮。

图1-9 配置 RIP 网络

(3) 配置设备 B

配置方式与设备 A 相同，不再赘述。

4. 验证配置

在 Host A 上使用 ping 命令验证 Host B 可达。

目 录

1 OSPF ····· 1-1
1.1 OSPF 简介 ····· 1-1
1.2 OSPF 的特点 ····· 1-1
1.2.1 OSPF 的 router-id ····· 1-2
1.2.2 OSPF 的区域划分 ····· 1-2
1.2.3 OSPF 的路由器类型 ····· 1-2
1.2.4 OSPF 的路由类型 ····· 1-3
1.2.5 OSPF 的网络类型 ····· 1-3
1.2.6 OSPF 的报文类型 ····· 1-4
1.2.7 协议规范 ····· 1-4
1.3 OSPF 配置 ····· 1-4
1.4 OSPF 网络配置 ····· 1-5
1.5 OSPF 接口配置 ····· 1-6
1.6 配置举例 ····· 1-8
1.6.1 OSPF 配置举例 ····· 1-8

1 OSPF

1.1 OSPF简介

OSPF（Open Shortest Path First，开放最短路径优先）是 IETF（Internet Engineering Task Force，互联网工程任务组）组织开发的一个基于链路状态的内部网关协议。目前针对 IPv4 协议使用的是 OSPF Version 2。

本节介绍配置 OSPF 所需要理解的知识，具体包括：

- OSPF 的特点
- OSPF 的报文类型
- OSPF 的区域划分
- OSPF 的路由器类型
- OSPF 的路由类型
- OSPF 的网络类型
- OSPF 的协议规范

说明

本章所介绍的配置都是指 OSPF version 2。

1.2 OSPF的特点

OSPF 具有如下特点：

- 可适应大规模网络：支持各种规模的网络，最多可支持几百台路由器。
- 路由变化收敛快：在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。
- 无路由自环：由于 OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- 支持区域划分：允许自治系统的网络被划分成区域来管理。路由器链路状态数据库的减小降低了内存的消耗和 CPU 的负担；区域间传送路由信息的减少降低了网络带宽的占用。
- 支持等价路由：支持到同一目的地址的多条等价路由。
- 支持路由分级管理：使用 4 类不同的路由，按优先顺序来说分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由。
- 支持验证：支持基于区域和接口的报文验证，以保证报文交互和路由计算的安全性。
- 组播发送：在某些类型的链路上以组播地址发送协议报文，减少对其它设备的干扰。

1.2.1 OSPF 的 router-id

路由器标识是一个 32 位数字，使其用来独一无二的识别 AS 中的路由器。

OSPF 协议需要路由器的 Router-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，会自动选出一个 Router-ID。通常路由器先挑选 IP 地址最大的环回地址。若无环回地址，则在接口状态为 up 的物理接口中，选取最大的 IP 地址作为 Router-ID。也可以指定一个 Router-ID，并且指定的 Router-ID 优先级最高。

1.2.2 OSPF 的区域划分

随着链路状态数据库的增大，计算 SPF 所需的时间也增加了，将网络分成较小的区域，并要求路由器与同一区域的路由器交换链路状态。这样传播的信息减少了。

1. 优点：

- 降低 CPU 的负担；
- 减小 LSDB 的内存开销；
- LSA 相关计算和 Flooding 负担均降低。

2. 划分要求

- 为了控制开销和便于管理 OSPF，支持将整个自治系统划分成域来管理，并且划分为骨干域和边缘域。
- 原则上要求每个非骨干区域要和骨干域直接相连，骨干域要求连通性强、带宽高。
- 当一台路由器配置两个以上的域时，必须有一个是骨干域。

3. 区域类型

骨干区域：所有的域间通信流量都必须通过骨干区域，非骨干区域之间不能直接交换数据包，区域 0（或 0.0.0.0）是骨干区域保留的区域 ID 号。

(1) 标准区域：一个标准区域可以接收链路更新信息和汇总路由。

(2) 末梢区域(stub area)：只与一个区域相连的非骨干区域，不接受外部自治系统的 LSA（类型 5），区域内路由器会把去往外部网络的路由基于缺省路由（目的地址是 0.0.0.0）发送出去。

(3) 完全末梢区域(totally stub area)：不接受类型 3、类型 4 和类型 5 的 LSA ，区域内路由器会把去往其它区域的路由基于缺省路由（目的地址是 0.0.0.0）发送出去。

(4) 非完全末梢区域(Not-so-stubby-area，NSSA)：该区域是 Stub 区域的变形，与 Stub 区域的区别在于 NSSA 区域允许引入自治系统外部路由，由 ASBR 发布 Type7 LSA 通告给本区域。当 Type7 LSA 到达 NSSA 的 ABR 时，由 ABR 将 Type7 LSA 转换成 Type5 LSA，传播到其它区域。

1.2.3 OSPF 的路由器类型

OSPF 路由器根据在 AS 中的不同位置，可以分为以下四类：

- 区域内路由器（Internal Router）

  该类路由器的所有接口都属于同一个 OSPF 区域。

- 区域边界路由器 ABR

  该类路由器可以同时属于两个以上的区域，但其中一个必须是骨干区域。ABR 用来连接骨干区域和非骨干区域，它与骨干区域之间既可以是物理连接，也可以是逻辑上的连接。

- 骨干路由器（Backbone Router）

  该类路由器至少有一个接口属于骨干区域。因此，所有的 ABR 和位于 Area0 的内部路由器都是骨干路由器。

- 自治系统边界路由器 ASBR

  与其它 AS 交换路由信息的路由器称为 ASBR。ASBR 并不一定位于 AS 的边界，它有可能是区域内路由器，也有可能是 ABR。只要一台 OSPF 路由器引入了外部路由的信息，它就成为 ASBR。

1.2.4 OSPF 的路由类型

OSPF 使用 4 类不同的路由，按优先级由高到低排列如下：

- 区域内路由
- 区域间路由
- 第一类外部路由
- 第二类外部路由

区域内和区域间路由描述自治系统内部的网络结构；外部路由则描述了如何选择到自治系统以外的路由。第一类外部路由是指接收的是 IGP 路由（例如 RIP、STATIC），由于这类路由的可信程度较高，所以，计算出的外部路由的花费与自治系统内部的路由花费的数量级相同，并且与 OSPF 自身路由的花费具有可比性，即到第一类外部路由的花费值＝本路由器到相应的 ASBR 的花费值加 ASBR 到该路由目的地址的花费值。第二类外部路由器是指接收的是 EGP 路由，由于这类路由的可信度比较低，所以 OSPF 协议认为，从 ASBR 到自治系统之外的花费远远大于在自治系统之内到达 ASBR 的花费，计算路由花费时主要考虑前者。即第二类外部路由的花费值等于 ASBR 到该路由目的地址的花费值。如果该值相等，再考虑本路由器到相应的 ASBR 的花费值。

1.2.5 OSPF 的网络类型

缺省情况下，按不同介质可划分成下列三种网络：广播网络（以太网，令牌环网、FDDI），非广播多路访问网络（帧中继、X.25），点到点网络（HDLC、PPP）。对以上任一类网络都可以进行 OSPF 配置。可以不考虑缺省的介质类型，选择配置 OSPF 网络类型。利用这一点，可将非广播多路访问网络配置为广播网络，如 X.25 和帧中继允许 OSPF 在其上以广播型网络运行，这就不用再去配置邻居。可将广播网络配置为非广播多路访问网络，例如当网络中有不支持组播传送地址的路由器时。对于不具有广播和组播能力的网络，必须配置对端邻居来指定发送 hello 报文，并可以指定邻居的优先级和轮询时间间隔。

点到多点时具有一个或者多个邻居的编号的点到点接口，它建立多主机路由。与非广播多路访问和点到点网络相比，点到多点网络具有以下优点：一到多接口更易于配置，因为它不需要配置邻居命令，只需要一个 IP 子网，所以不必分配路由选择。不需要全网络拓扑结构，开销较小。

说明

设备只支持广播型网络和点对点型网络。

1.2.6 OSPF 的报文类型

OSPF 协议报文直接封装为 IP 报文，协议号为 89。

OSPF 有五种类型的协议报文：

- Hello 报文：发现及维持邻居关系，选举 DR，BDR；
- DD（Database Description，数据库描述）报文：相邻路由器之间发 DD 报文，报告对方自己所拥有的路由信息内容，包括 LSDB 中每一条 LSA 摘要(摘要是指 LSA 的 HEAD，通过该 HEAD 可以唯一标识一条 LSA)，这样做的目的是为了减少路由器之间传递信息的量，因为 LSA 的 HEAD 只占一条 LSA 的整个数据量的一小部分。根据 HEAD，对端路由器就可以判断出是否已经有了这条 LSA。
- LSR（Link State Request，链路状态请求）报文：向对方请求所需的 LSA。两台路由器互相交换 DD 报文之后，得知对端的路由器有哪些 LSA 是本地的 LSDB 所缺少的，这时需要发送 LSR 报文向对方请求所需的 LSA。
- LSU（Link State Update，链路状态更新）报文：向对方发送其所需要的 LSA。
- LSAck（Link State Acknowledgment，链路状态确认）报文：用来对收到的 LSA 进行确认。

1.2.7 协议规范

与 OSPF 相关的协议规范有：

- RFC 1765：OSPF Database Overflow
- RFC 2328：OSPF Version 2
- RFC 3101：OSPF Not-So-Stubby Area (NSSA) Option
- RFC 3137：OSPF Stub Router Advertisement
- RFC 3630：Traffic Engineering Extensions to OSPF Version 2
- RFC 4811：OSPF Out-of-Band LSDB Resynchronization
- RFC 4812：OSPF Restart Signaling
- RFC 4813：OSPF Link-Local Signaling

1.3 OSPF配置

通过菜单“网络配置 > 路由管理 > OSPF 信息”，进入如图 1-1 所示页面。在该页面上，可以配置 OSPF 路由器 ID、是否发布缺省路由及路由重发布信息。这些信息的详细说明如表 1-1 所示。

图1-1 OSPF 配置

表1-1 OSPF 各配置项说明

标题项	说明
启用	启用或禁用OSPF策略，勾选为启用，不勾选为禁用。禁用后会删除OSPF网络配置。
路由器ID	OSPF路由器ID
缺省路由	是否发布默认路由，可选发布、不发布及强制发布
直连路由	设置是否重发布直连路由，并设置直连路由的cost
静态路由	设置是否重发布静态路由，并设置静态路由的cost
RIP路由	设置是否重发布RIP路由，并设置RIP路由的cost

说明

- 通常路由器先挑选 IP 地址最大的环回地址作为 Router-ID。若无环回地址，则在接口状态为 up 的物理接口中，选取最大的 IP 地址作为 Router-ID。也可以指定一个 Router-ID，并且指定的 Router-ID 优先级最高。
- 缺省路由：如果路由表中有默认路由，并且想要发布出去，选中“发布”即可；如果路由表中没有默认路由，想要发布默认路由则需要选中“强制发布”。

1.4 OSPF网络配置

(1) 通过点击图 1-1 中的“OSPF 网络”，进入如图 1-2 所示页面。该页显示了已经配置的 OSPF 网络，在该页也可以删除已经配置的 OSPF 网络。

图1-2 OSPF 已配置网络

(2) 点击图 1-2 中的<新建>按钮，进入如图 1-3 所示页面，在该页填入要发布的 OSPF 网络及区域。

图1-3 OSPF 网络配置

1.5 OSPF接口配置

(1) 点击图 1-4 中的“OSPF 接口”，进入所示图 1-4 页面。该页面显示了已经配置的接口信息，具体信息说明如表 1-2 所示。

图1-4 已经配置的接口信息

表1-2 RIP 扩展各项含义

标题项	说明
接口名称	已经配置的接口名称
认证算法	接口所使用的加密方式，有明文、密文及不认证
操作	点击可以对该配置进行修改，点击可以删除该配置

(2) 点击图 1-4 中的<新建>按钮，进入如图 1-5 所示页面。该页面可以配置接口相关的 OSPF 信息，具体信息说明如表 1-3 所示。

图1-5 OSPF 接口配置

表1-3 OSPF 接口各项配置含义

标题项	说明
接口	选择要配置接口
优先级	设置接口的优先级
发送开销	设置接口发送数据包的开销
网络类型	设置网络类型
认证	设置认证方式：不认证、明文认证、密文认证
hello间隔	设置hello报文的时间间隔
重传间隔	设置重传间隔
Dead间隔	设置邻居失效间隔
发送延迟	设置报文的发送延迟时间

1.6 配置举例

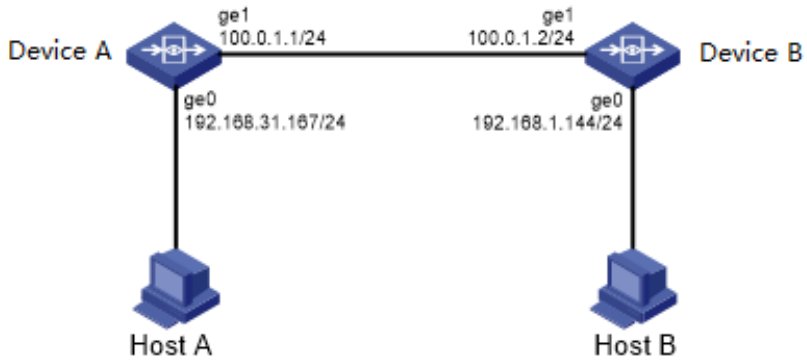
1.6.1 OSPF 配置举例

1. 组网需求

按照图 1-6 所示，配置 IP 地址，要求设备 A 和设备 B 上启用 OSPF，设备 A 设备能学到 192.168.1.0/24 网段的路由，设备 B 能学到 192.168.31.0/24 网段的路由。

2. 组网图

图1-6 OSPF 配置案例组网图



3. 配置步骤

(1) 按照组网图组网。

(2) 配置设备 A。

- 通过菜单“网络配置 > 路由管理 > OSPF 信息”，进入 OSPF 配置页面，如图 1-7 所示，设置相关数据，点击<提交>。

图1-7 OSPF 配置

- 点击图 1-7 中的 OSPF 网络”，进入如图 1-2 所示页面，点击新建，进入如图 1-8 所示页面，并点击<提交>按钮。

图1-8 配置 RIP 网络

(3) 配置设备 B

设备 B 的配置方式与设备 A 相同，在此不再赘述。

4. 验证配置

在 Host A 上使用 ping 命令验证 Host B 可达。

目 录

1 策略路由 ····· 1-1
1.1 概述 ····· 1-1
1.2 策略路由表 ····· 1-1
1.3 策略路由配置 ····· 1-1
1.4 移动策略路由 ····· 1-3
1.5 配置举例 ····· 1-3
1.5.1 策略路由配置举例 ····· 1-3
1.5.2 组网需求 ····· 1-3
1.5.3 组网图 ····· 1-4
1.5.4 配置步骤 ····· 1-4
1.5.5 验证配置 ····· 1-5

1 策略路由

1.1 概述

策略路由，也叫做基于策略的路由，是指在决定一个 IP 包的下一跳转发地址时，不是简单的根据目的或源 IP 地址来决定，而是综合考虑多种因素决定。它转发分组到特定网络需要基于预先配置的策略，这个策略可能指定从一个特定的网络发送的通信应该被转发到一个指定的接口。策略路由支持 IPv4 和 IPv6 的使用场景。

1.2 策略路由表

通过菜单“网络配置 > 路由管理 > 策略路由”，进入如图 1-1 所示页面。在该页面上，可以查看已经配置的策略路由信息。这些信息的详细说明如表 1-1 所示。

图1-1 策略路由表

表1-1 策略路由表的显示信息

标题项	说明
ID	策略路由的ID
入接口	报文的入接口
源地址	源地址对象名称，地址对象或对象组
目的地址	目的地址对象名称，地址对象或对象组
用户	用户对象名称
服务	服务对象名称
应用	应用对象名称
下一跳/出接口	报文转发的下一跳/出接口
操作	点击可以对该条策略路由进行修改，点击可以删除该条策略路由

1.3 策略路由配置

通过点击图 1-1 中的“新建”，进入如图 1-2 所示页面。各配置项含义如表 1-2 所示。

图1-2 策略路由配置页面

表1-2 策略路由配置项含义

标题项	说明
入接口	报文的入接口
源地址	源地址对象名称，地址对象或地址对象组，单击后面的<新建>可以创建地址对象/地址对象组对象。
目的地址	目的地址对象名称，地址对象或地址对象组，单击后面的<新建>可以创建地址对象/地址对象组对象。
用户	用户对象名称，单击后面的<选择用户>可以在用户组中选择或排除用户。
服务	服务对象名称，单击后面的<新建>按钮，可以创建自定义服务或服务组。
应用	应用对象名称
时间	策略路由生效时间，单击后面的<新建>按钮，可以创建时间对象。
下一跳信息	可以选择下一跳地址，也可以选择出接口。下一跳地址可以配置为IPv4或IPv6地址。
权重	该策略路由的权重值

1.4 移动策略路由

通过点击图 1-1 中的“优先级”，进入如图 1-3 所示页面。各配置项含义如表 1-3 所示。

图1-3 移动策略路由

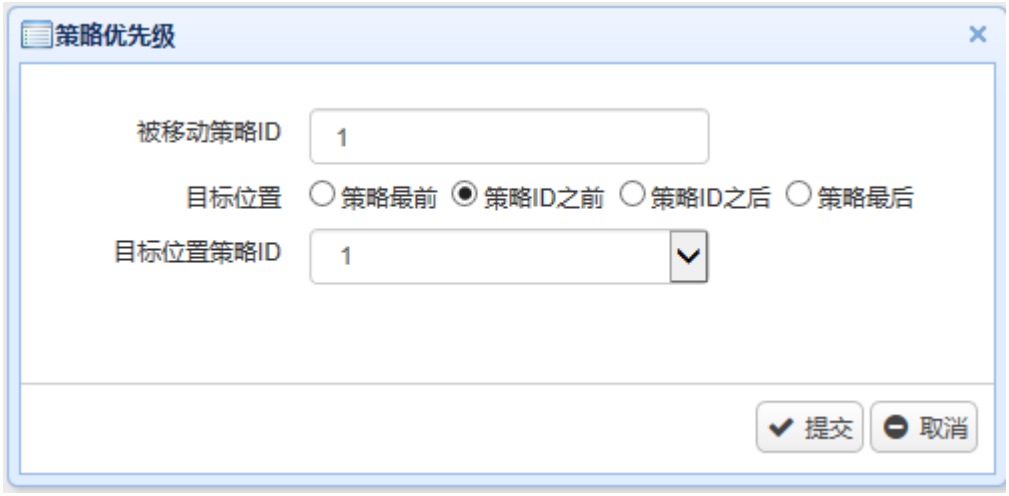


表1-3 移动策略路由配置项含义

标题项	说明
被移动策略ID	被移动策略ID
目标位置	要移动到的位置，一共四个位置：策略最前、策略ID之前、策略ID之后、策略最后
目标位置策略ID	目标位置策略ID

1.5 配置举例

1.5.1 策略路由配置举例

1.5.2 组网需求

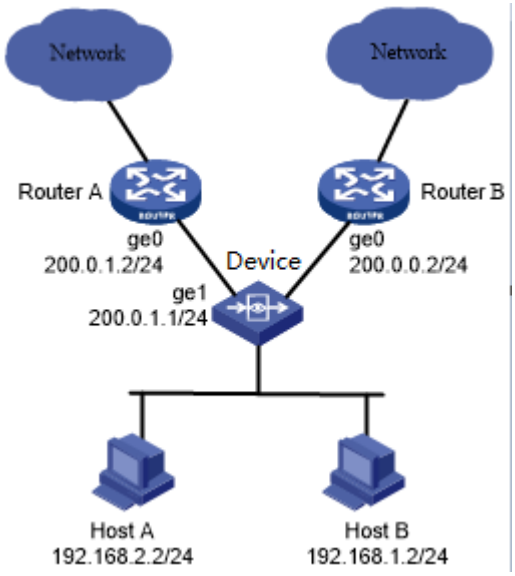
各设备接口及主机的 IP 地址和掩码如图 1-4 所示。

- 将来自 192.168.1.0/24 网段的数据包路由至设备 200.0.0.2 上。
- 将来自 192.168.2.0/24 网段的数据包路由至设备 200.0.1.2 上。

通过这样的配置可以有选择的限制不同的 IP 用户访问不同的网络或使用不同的网络出口。

1.5.3 组网图

图1-4 策略路由配置案例组网图



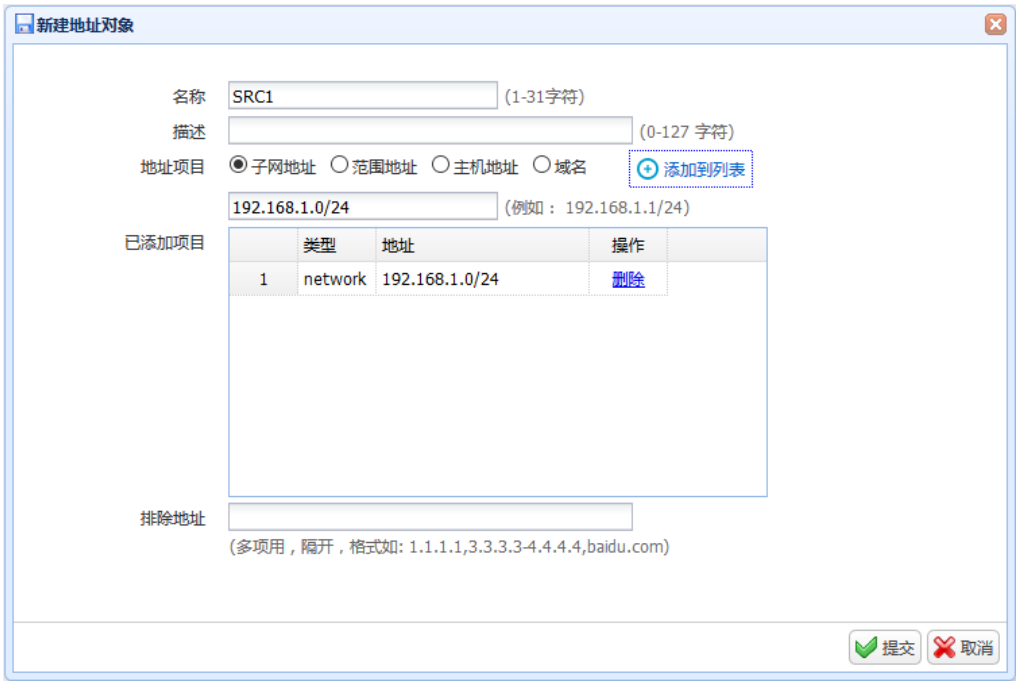
1.5.4 配置步骤

(1) 按照组网图组网

(2) 通过菜单“网络配置 > 路由管理 > 策略路由”，点击<新建>，进入如图 1-2 所示的页面。

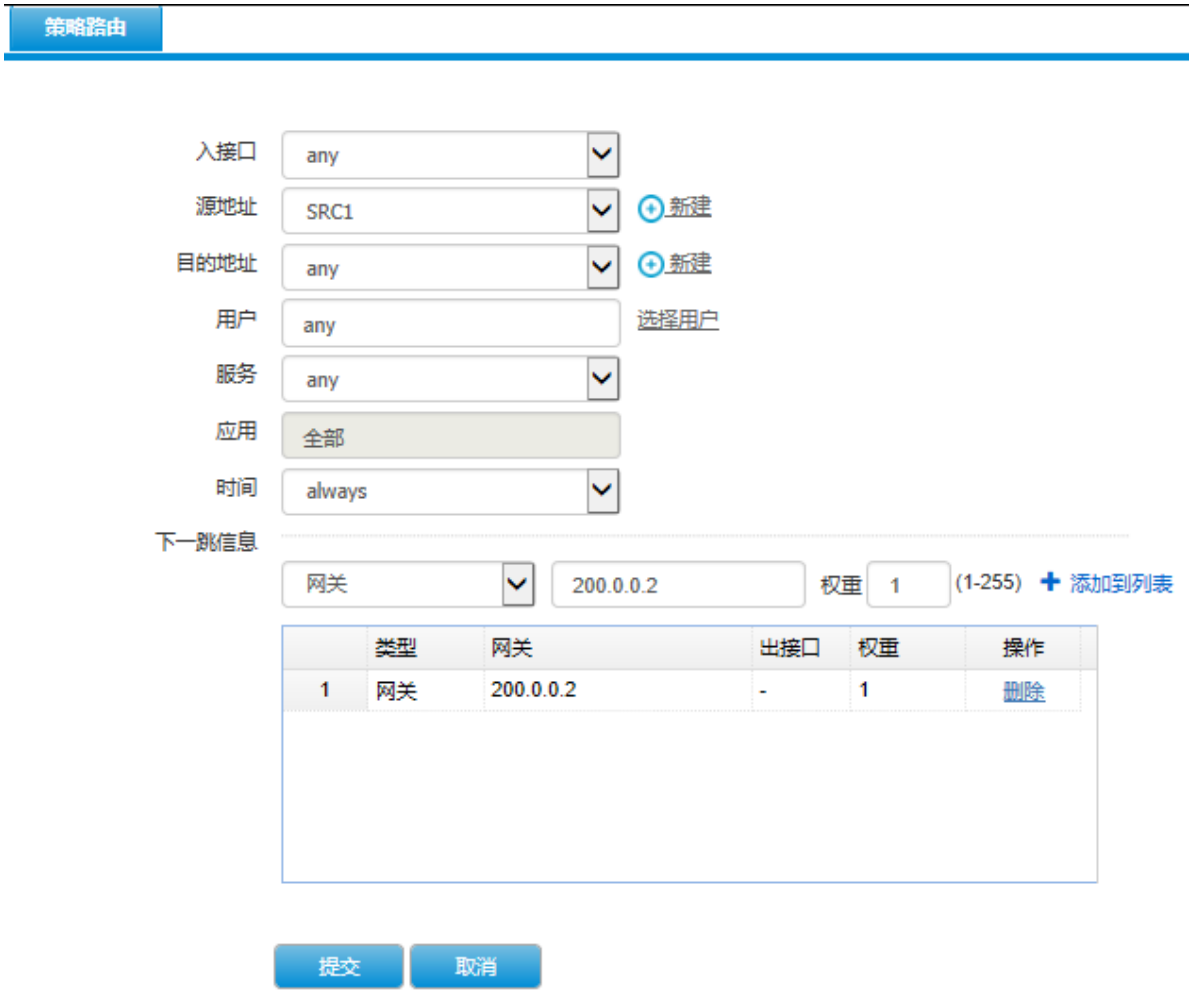
(3) 点击源地址那一栏后面的<新建>，建立 192.168.1.0/24 的地址对象，如图 1-5 所示。

图1-5 地址对象配置



(4) 点击<提交>按钮，进入策略路由配置页面，并如图 1-6 所示填写下一跳信息，并点击<提交>按钮提交该页配置。

图1-6 配置策略路由



(5) 同样方式配置 192.168.2.0/24 网段的策略路由。

1.5.5 验证配置

查看策略路由表，查看是否已经有已经配置的策略路由，如图 1-7 所示。

图1-7 验证策略路由配置

		ID	入接口	源地址	目的地址	用户	服务	应用	下一跳/出接口
1		1	any	SRC1	any	any	any	全部	200.0.0.2
2		2	any	SRC2	any	any	any	全部	200.0.1.2

目 录

1 ISP 路由 ····· 1-1
1.1 概述 ····· 1-1
1.2 配置 ISP 地址库 ····· 1-1
1.3 配置 ISP 路由 ····· 1-2

1 ISP 路由

1.1 概述

很多用户通常会申请多条线路进行流量负载均衡。然而，一般的均衡是不会根据流量的流向，做均衡的，如果网通的服务器通过电信访问，网速就会很慢。安全网关针对该问题，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。

1.2 配置ISP地址库

配置 ISP 路由，用户首先需要将子网条目添加到一个 ISP 地址库，然后才可以配置以 ISP 地址库名称为目的地的 ISP 路由。用户可以自定义 ISP 地址库，也可以使用预定义的 ISP 的地址库。安全网关提供了四个预定义 ISP 地址库，分别是中国电信（ChinaTelecom）、中国联通（Chinaunicom）、教育网（ChinaEducation）、中国移动（ChinaMobile）。配置步骤如下：

(1) 通过菜单“网络配置 > 路由管理 > ISP 路由”，进入如图 1-1 所示页面。在该页面上，可以查看预定义的 ISP 地址库和自定义的地址库信息。

图1-1 ISP 地址库

(2) 点击图 1-1 中的<新建>按钮，进入 ISP 地址库的配置页面，如图 1-2 所示。各配置项含义如表 1-1 所示。

图1-2 新建 ISP 地址库

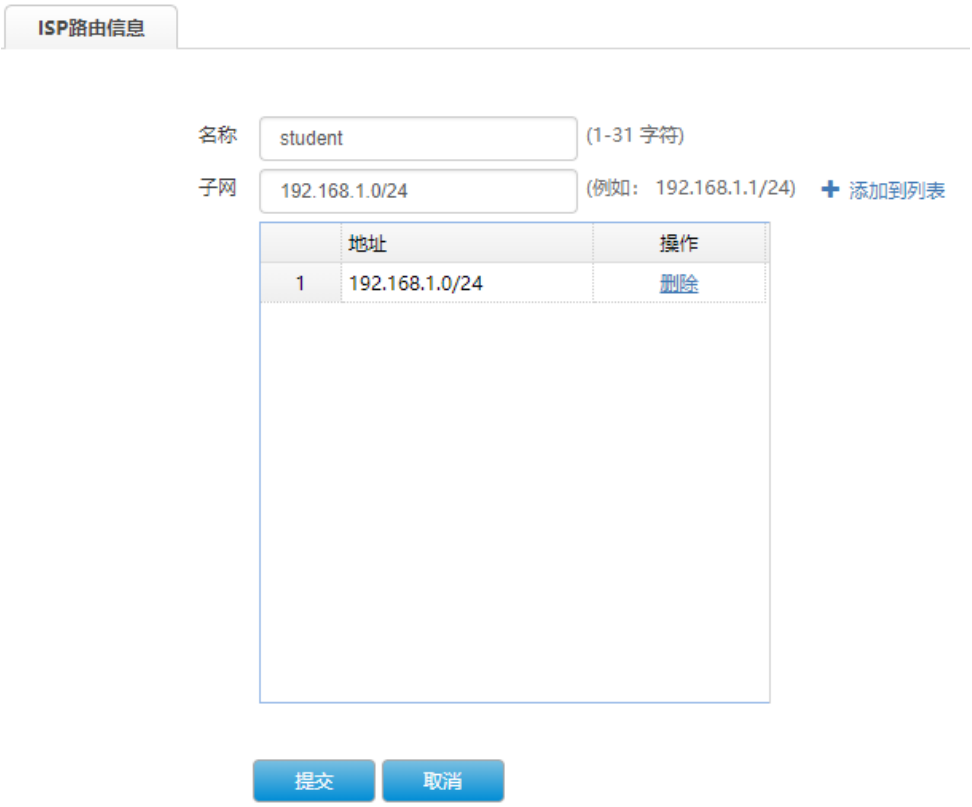


表1-1 ISP 地址库配置项含义

标题项	说明
名称	设置ISP地址库名称
子网	设置ISP地址库中的子网网段

说明

- 用户自定义的 ISP 地址库名称不能与预定义的相同。
- 用户自定义的 ISP 地址库，每个 ISP 最多有 200 个地址网段。
- 用户可以编辑自定义的 ISP 地址库，不可以编辑预定义的。

1.3 配置ISP路由

(1) 通过点击图 1-1 中的“ISP 路由”页签，进入如图 1-3 所示页面。各项含义如表 1-2 所示。

图1-3 ISP 路由页面

表1-2 ISP 路由各项含义

标题项	说明
名称	ISP路由所使用地址库名称
下一跳/出接口	ISP路由的下一跳/出接口
权重	ISP路由的权重，范围是<1-255>
优先级	ISP路由的优先级，范围是<1-255>
地址探测	和ISP路由联动的地址探测，如果已经配置和探测联动，点击地址探测名称可以修改和路由联动的地址探测
操作	点击可以删除该ISP路由

说明

- 权重：在多下一跳负载均衡时，当优先级相同，根据源地址哈希值按照权重比值分摊流量。
- 优先级：路由类型的优先级，该值越小，优先级越高。
- ISP 路由和静态路由的优先级相同，如果出现相同的目的网段同时同时配置 ISP 路由和静态路由的下一跳不同，流量负载分担

(2) 点击图 1-3 中<新建>按钮，进入 ISP 路由配置页面，如图 1-4 所示，各配置项含义如表 1-3 所示。

图1-4 ISP 路由配置

表1-3 ISP 路由各配置项含义

标题项	说明
ISP名称	ISP路由所使用地址库名称
下一跳/出接口	ISP路由的下一跳/出接口
权重	ISP路由的权重，范围是<1-255>
优先级	ISP路由的优先级，范围是<1-255>
地址探测	配置和ISP路由联动的地址探测，单击后面的<新建>按钮可以创建地址探测或地址探测组。

说明

- 权重：在多下一跳负载均衡时，权重越大，命中的概率就越大。
- 距离：路由类型的优先级，该值越小，优先级越高。

目 录

1 IPsec ····· 1-1
1.1 IPsec 概述 ····· 1-1
1.2 配置 IPsec ····· 1-1
1.2.1 配置概述 ····· 1-1
1.2.2 配置 IKE 协商策略 ····· 1-2
1.2.3 配置 IPsec 协商策略 ····· 1-5
1.2.4 配置 IPsec 安全策略 ····· 1-7
1.2.5 配置 IPsec 隧道接口 ····· 1-7
1.3 IPsec VPN 的查看和管理 ····· 1-8
1.3.1 查看 IPsec SA ····· 1-8
1.3.2 查看 IKE SA ····· 1-9
1.4 商密 IPSec 典型配置举例 ····· 1-10
1.4.1 组网需求 ····· 1-10
1.4.2 组网图 ····· 1-10
1.4.3 配置步骤 ····· 1-10
1.4.4 验证配置结果 ····· 1-18
1.5 国密 IPSec 典型配置举例 ····· 1-19
1.5.1 组网需求 ····· 1-19
1.5.2 组网图 ····· 1-19
1.5.3 配置步骤 ····· 1-19
1.5.4 验证配置结果 ····· 1-30
2 IPsec 快速配置 ····· 2-32
2.1 IPsec 快速配置概述 ····· 2-32
2.2 创建 IPsec 快速配置 ····· 2-33
2.2.1 配置概述 ····· 2-33
2.2.2 节点基本信息配置 ····· 2-33
2.2.3 保护网段配置 ····· 2-35
2.2.4 高级选项配置 ····· 2-36
2.3 IPsec 状态监控 ····· 2-38
2.3.1 查看 IPsec 监控 ····· 2-38
2.4 IPSec 典型配置举例 ····· 2-39
2.4.1 组网需求 ····· 2-39

2.4.2 组网图 ····· 2-40
2.4.3 配置步骤 ····· 2-40
2.4.4 验证配置结果 ····· 2-42

1 IPsec

1.1 IPsec概述

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：

- 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 包并且丢弃。

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 配合工作也可以单独工作。
- 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）是缺省的密钥自动交换协议。

1.2 配置IPsec

1.2.1 配置概述

IPsec 配置的推荐步骤如表 1-1 所示。

表1-1 IPsec 配置的推荐步骤

配置任务	说明	详细配置
配置IKE协商策略	必选	1.2.2
配置IPsec协商策略	必选	1.2.3
配置IPsec隧道接口	必选	1.2.5

1.2.2 配置 IKE 协商策略

在导航栏中选择“网络配置>VPN>IPsec-VPN> IPsec 第三方对接”，进入 IPsec 的显示页面，如图 1-1 所示。

图1-1 IPsec 显示页面

页面的详细说明如表 1-2。

表1-2 IPsec 显示页面的详细说明

项目	说明
名称	IKE的和对应的IPsec名称。
详细信息	IKE的详细信息。
操作	可以对相应IPsec进行的操作。

单击<新建>按钮，在下拉菜单中选择<新建 IKE>，或者点击对应 IKE 的右侧<编辑>按钮，进入 IKE 的配置页面，如图 1-2 所示。

图1-2 IKE 新建页面

页面的详细说明如表 1-3 所示。

表1-3 IKE 配置的详细说明

项目	说明
网关名称	IKE的名称
本地源接口/本地源IP地址/无	当有多出口时，需要指定用于建立IPsec的本端IP地址。如果指定的是本地源接口，则使用该接口上的主IP作为本端IP地址。 说明：对于本地源IP和无的配置，接口down无法判断要清除那个SA，所以统一处理逻辑为接口down不自动清SA，通过DPD机制来检测链路状态即可，DPD保活失败，会自动清除SA
对端网关	指定对端网关，可以有静态IP、域名、动态三种选择。
IP地址/域名	根据对端网关选择的类型，可以输入对端网关的IP地址或者域名。
认证方式	指定一阶段认证所采用的方式，有预共享密钥、数字证书和国密认证三种选择。
预共享密钥/证书、CA证书、国密证书	根据认证方式选择的类型，预共享密钥、CA证书或者国密证书。

点击<高级选项>，可以显示出更多内容，如图 1-3 所示。

图1-3 IKE 新建页面高级选项

页面的详细说明如表 1-4 所示。

表1-4 IKE 配置高级选项的详细说明

项目	说明
IKE协商交互方案	添加一阶段协商所需要的加密提案，最多可以添加3个。默认加密方式为AES256_SHA2_256。
DH组	指定DH交换组。
密钥周期	密钥的生成周期。
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。
本端ID	支持IP地址，FQDN和User-FQDN三种格式。其中FQDN和User-FQDN只能用于野蛮模式。
对端ID	支持IP地址，FQDN和User-FQDN三种格式。其中FQDN和User-FQDN只能用于野蛮模式。 用于校验对端的ID，以匹配对应的IKE。
对等体状态探测	即DPD监测，可以开启该功能，用以探测对端的存活状况。 对于IPSEC分支非常多的场景，如有几千个甚至上万个分支，不建议开启DPD检测，否则

项目	说明
	中心端的设备会因为处理大量DPD报文而严重消耗CPU资源
DPD检测间隔	发送DPD报文的间隔。
DPD失败重试间隔	如果前一次发送的DPD报文未得到回应，则使用重试间隔来发送下一次DPD报文。一般DPD失败重试间隔小于DPD检测间隔，用于快速地确认对端是否存活。
DPD失败重试次数	在重试了指定次数后，仍未得到对端的回应，则认为对端已断开连接。
扩展认证	开启该功能后，需要在用户管理页面添加用户，具体步骤可参考用户管理模块。
模式配置	给远程接入的用户分配地址及下发DNS、WINS服务器。
地址池	给远程接入的用户分配地址的地址对象。
拨号用户DNS	给远程接入的用户分配的DNS。
拨号用户WINS	给远程接入的用户分配的WINS。

输入完毕后，点击<提交>按钮，应用配置。

在 IPsec 显示页面，点击 IKE 右侧的<删除>按钮，可以删除对应的 IKE。

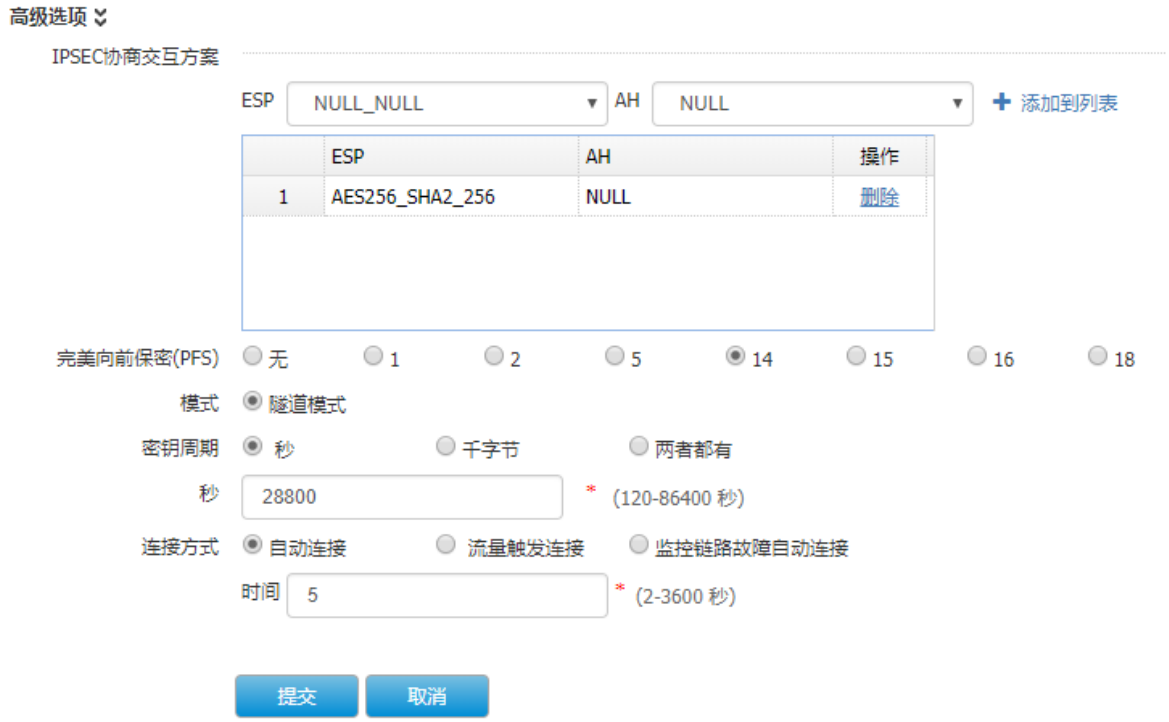
1.2.3 配置 IPsec 协商策略

在导航栏中选择“网络配置 > VPN > IPsec-VPN > Ipsec 第三方对接”，进入 IPsec 配置的显示页面，单击<新建 IPsec>按钮，或者点击对应 IPsec 的右侧<编辑>按钮，进入 IPsec 协商策略的配置页面，如图 1-4 所示。

图1-4 IPsec 新建页面

点击下方<高级选项>按钮可以显示更多的配置选项，如图 1-5 所示。

图1-5 IPsec 协商策略高级选项配置页面



页面的详细说明如表 1-5 所示。

表1-5 IPsec 协商策略配置的详细说明

项目	说明
通道名称	IPsec协商策略名称。
IKE	选择一个已经新建的IKE。
IPsec协商交互方案	添加二阶段协商所需要的加密提案，最多可以添加4个。ESP和AH不允许全为空。
完美向前保密（PFS）	指定完美向前保密组。
模式	IPSEC加密的封装模式，目前只支持隧道（tunnel）模式。
密钥周期	指定IPSEC SA最大有效时间，有时间、流量、时间+流量三种选择。
自动连接	是否开启自动连接功能，如果开启此选择需同时设定一个自动重连时间间隔。
流量触发连接	开启此功能，不会建立IPsec隧道，在有流量通过的情况，才会建立IPsec隧道。
监控链路故障自动连接	此功能必须设置时间为自动连接的时间； 主链路：需要选择监控的主链路； 切换延迟时间：主链路选择后需要设置主链路故障后切换到本链路的时长。

输入完毕后，点击<提交>按钮，应用配置。

在 IPsec 显示页面，点击 IPsec 右侧的<删除>按钮，可以删除对应的 IPsec。

1.2.4 配置 IPsec 安全策略

在导航栏中选择“策略配置 > 控制策略”，进入控制策略的显示页面，单击<新建>按钮，进入控制策略新建页面，行为选择“允许”，点击<提交>按钮，应用配置。

1.2.5 配置 IPsec 隧道接口

在导航栏中选择“网络配置 > VPN > IPsec-VPN > Ipsec 第三方对接 > IPsec 隧道接口”，进入 IPsec 隧道接口的显示页面，如图 1-6 所示。

图1-6 IPsec 隧道接口显示页面

页面的详细说明如表 1-6。

表1-6 IPsec 隧道接口显示页面的详细说明

项目	说明
IPsec接口	IPsec接口名称。
IPv4地址	隧道接口的IPv4地址。
IPsec	隧道接口对应的IPsec协商策略。
地址项目	感兴趣流对应源网段和目的网段。
操作	可以对相应IPsec隧道接口执行的操作。

单击页面上方<新建>按钮，或者点击对应隧道接口的右侧<编辑>按钮，进入 IPsec 隧道接口的配置页面，如图 1-7 所示。

图1-7 IPsec 隧道接口的新建页面

页面的详细说明如表 1-7。

表1-7 IPsec 隧道接口新建页面的详细说明

项目	说明
IPsec	IPsec隧道的编号，系统会自动推荐一个空闲的编号，也可自行填入。
IPv4地址	为tunnel接口指定一个IPv4地址。
IPsec	指定一个已经存在的IPsec协商策略。
地址项目	设置感兴趣流，输入源网段和目的网段，点击<添加到列表>，加入下方的列表中。

输入完毕后，点击<提交>按钮，应用配置。

在 IPsec 隧道接口显示页面，点击隧道接口右侧的<删除>按钮，可以删除对应的隧道接口。

1.3 IPsec VPN的查看和管理

1.3.1 查看 IPsec SA

在导航栏中选择“网络配置 > VPN > IPsec-VPN > Ipsec 第三方对接 > IPsec SA”，进入 IPsec SA 显示页面。页面中显示了已经新建的 IPsec SA。如图 1-8 所示。

图1-8 IPsec SA 显示页面

页面的详细说明如表 1-8。

表1-8 IPsec SA 显示页面的详细说明

项目	说明
名称	IPsec SA的名称。
对端网关	IPsec SA的对端网关。
本地网关	IPsec SA的本地网关。
状态	IPsec SA的状态： “连接”表示IPsec连接成功； “未连接”表示IPsec连接不成功，需要检查对接双方网络以及IPsec配置是否有问题。
过期时间/过期流量	IPsec SA的过期时间/过期流量。
流量（入/出）	IPsec SA的入流量/出流量。
源网络	IPsec SA的源网络。
目的网络	IPsec SA的目的网络。
操作	可以对相应IPsec SA进行的操作。单击“ ”可以查看IPsec SA的具体信息，例如状态、ESP、AH等； 单击“ ”可以清除当前IPsec SA的状态记录，设备会自动重新建立IPsec连接，不影响配置。

点击页面右侧的<删除>按钮，可以删除对应的 IPsec SA。

点击页面右侧的<详细>按钮，可以看到对应的 IPsec SA 的详细信息。

1.3.2 查看 IKE SA

在导航栏中选择“网络配置 > VPN > IPsec-VPN > Ipsec 第三方对接 > IKE SA”，进入 IKE SA 显示页面，页面中显示了已经新建的 IKE SA。如图 1-9 所示。

图1-9 IKE SA 显示页面

页面的详细说明如表 1-9。

表1-9 IKE SA 显示页面的详细说明

项目	说明
名称	IKE SA的名称。
对端网关	IKE SA的对端网关。
本地网关	IKE SA的本地网关。
状态	IKE SA的状态： “连接”表示IKE连接成功； “未连接”表示IKE连接不成功，需要检查对接双方网络以及IKE配置是否有问题。
过期时间	IKE SA的过期时间。
操作	可以对相应IKE SA进行的操作，可以清除此条IKE的状态记录，设备会自动重新建立IKE连接，不影响配置。

点击页面右侧的<删除>按钮，可以删除对应的 IKE SA。

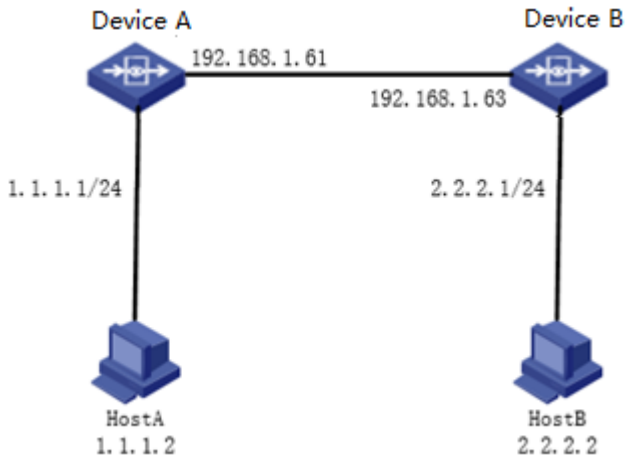
1.4 商密IPSec典型配置举例

1.4.1 组网需求

如下图 1-10 所示，在设备 A 和设备 B 之间使用商密标准建立一个安全隧道，对 Host A 代表的子网（1.1.1.0/24）与 Host B 代表的子网（2.2.2.0/24）之间的数据流进行安全保护。

1.4.2 组网图

图1-10 IPsec 举例组网图



1.4.3 配置步骤

(1) 新建 IKE 协商

对设备 A 的 IKE 配置如下图 1-11 所示。

图1-11 设备 A 的 IKE 配置

注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

对设备 B 的 IKE 配置如下图 1-12 所示。

图1-12 设备 B 设备 IKE 配置

注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

(2)　配置 IPsec 协商策略

对设备 A 的 IPsec 协商策略配置如下图 1-13 所示。

图1-13 设备 A 的 IPsec 协商策略配置

对设备 B 的 IPsec 协商策略配置如下图 1-14 所示。

图1-14 设备 B 的 IPsec 协商策略配置

(3) 新建所需地址对象

图1-15 设备 地址对象配置

		名称	内容(网络，范围，主机，域名)	排除地址	描述	引用	操作
4		ChinaTelecom	1.0.1.0/24, 1.0.2.0/23, 1.0.8.0/21, 1.0.32.0/19, 1.1.0.0/24, ...		中国电信	0	
5		ChinaEducation	1.51.0.0/20, 1.51.16.0/20, 1.51.32.0/19, 1.51.64.0/19, 1.51.96.0/20, ...		中国教育网	1	
6		ChinaMobile	36.128.0.0/12, 36.144.0.0/14, 36.148.0.0/16, 36.149.0.0/16, 36.150.0.0/15, ...		中国移动	0	
7		1_24	1.1.1.0/24			0	
8		2_24	2.2.2.0/24			0	

(4) 新建 IPSec 安全策略

图1-16 设备 A 的安全策略配置信息

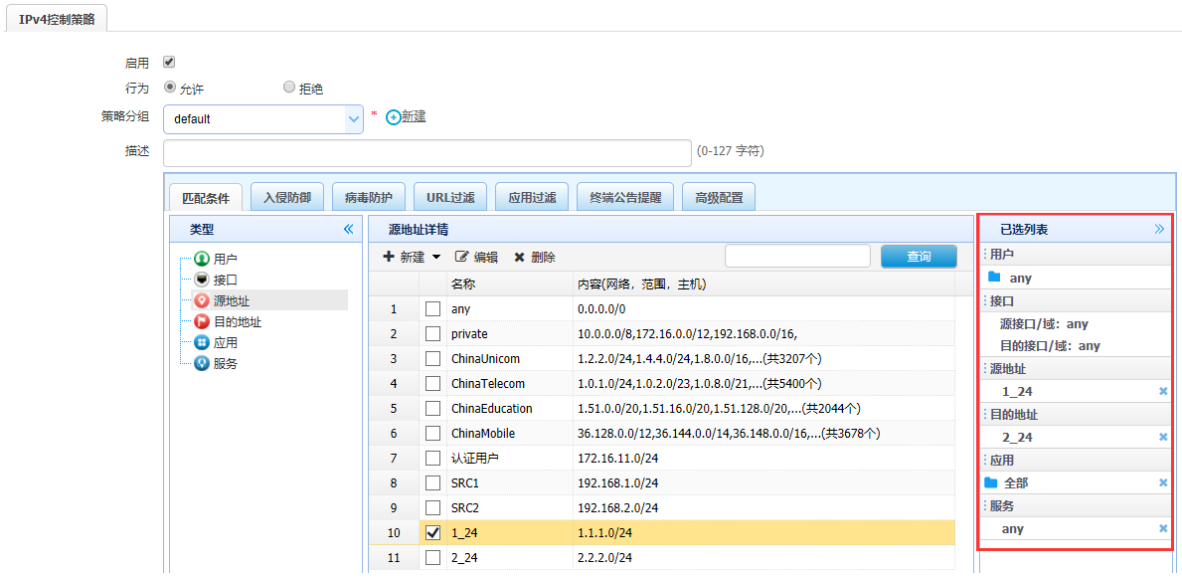
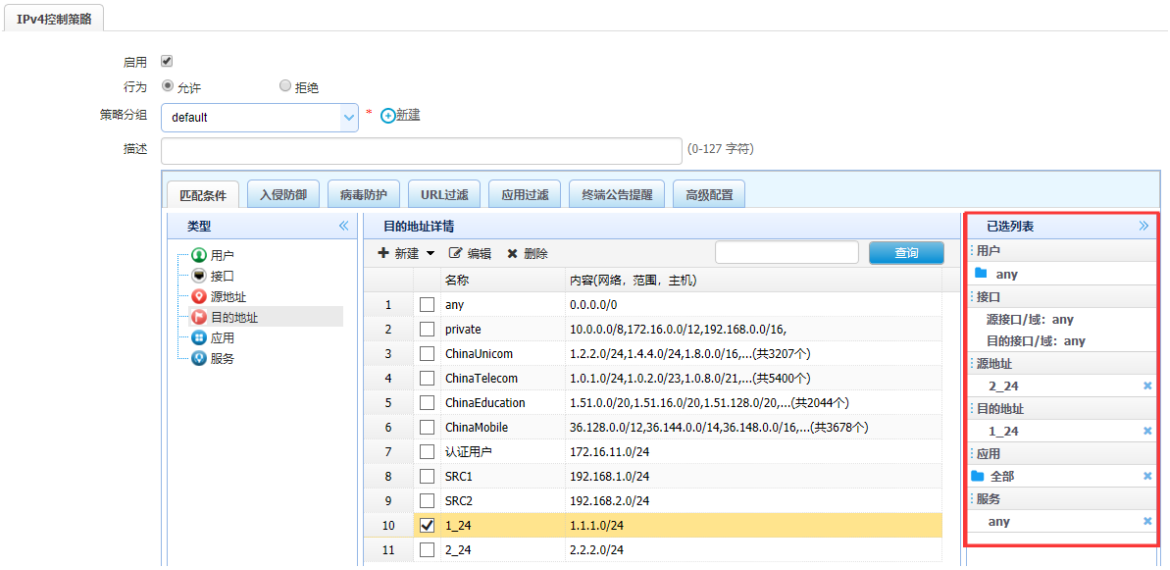


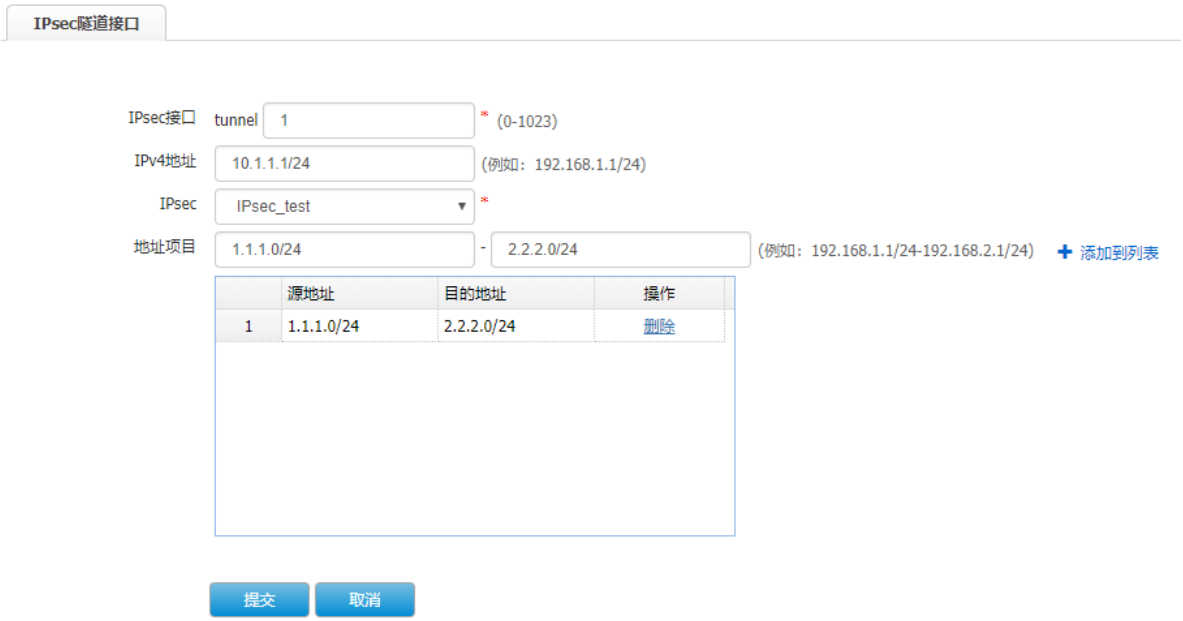
图1-17 设备 B 的安全策略配置信息



(5) 新建 IPSEC 隧道接口

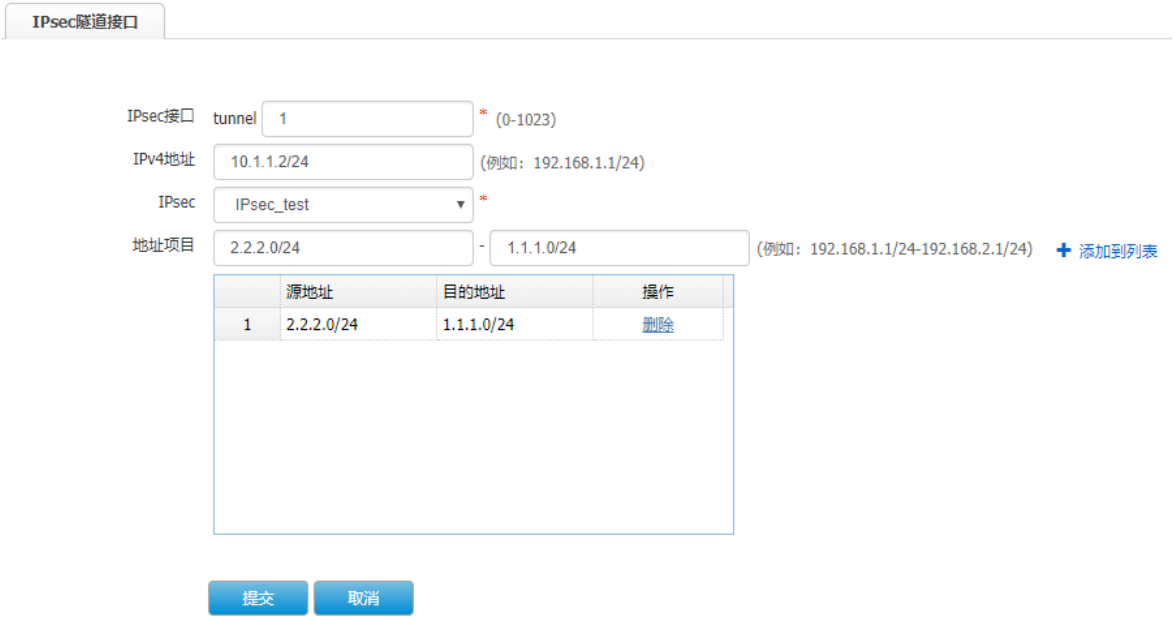
设备 A 的隧道接口如图 1-18 下所示。

图1-18 设备 A 的隧道接口配置



设备 B 的隧道接口如下图 1-19 所示。

图1-19 设备 B 的隧道接口配置



注：配置 IPsec 隧道时，隧道接口地址可选配置。是否配置隧道地址与怎样配置静态路由有关。配置隧道地址后路由可指定下一跳地址的方式去写。未配置隧道地址时需选用出接口的方式去写路由。

(6) 配置静态路由

需要将感兴趣流的路由指向 tunnel 口。

图1-20 设备 A 静态路由配置

出接口配置方式：

下一跳配置方式：

图1-21 设备 B 静态路由配置

出接口配置方式：

下一跳配置方式：

1.4.4 验证配置结果

在导航栏中选择“网络配置 > VPN > IPsec-VPN > IPsec 第三方对接 > IPsec SA”，查看 IPsec SA。

图1-22 设备 A 的 IPsec SA

IPsec 配置 | IPsec隧道接口 | IKE SA | IPsec SA

	名称	对端网关	本地网关	状态	过期时间/过期流	流量(入/出)	源网络	目的网络	操作
1	IPsec_test	192.168.1.63	192.168.1.61	连接	0s/0.0KB	0.00kb/0.00kb	1.1.1.0/24	2.2.2.0/24	

图1-23 设备 B 的 IPsec SA

IPsec 配置 | IPsec隧道接口 | IKE SA | IPsec SA

	名称	对端网关	本地网关	状态	过期时间/过期流	流量(入/出)	源网络	目的网络	操作
1	IPsec_test	192.168.1.61	192.168.1.63	连接中	0s/0.0KB	0.00kb/0.00kb	1.1.1.0/24	2.2.2.0/24	

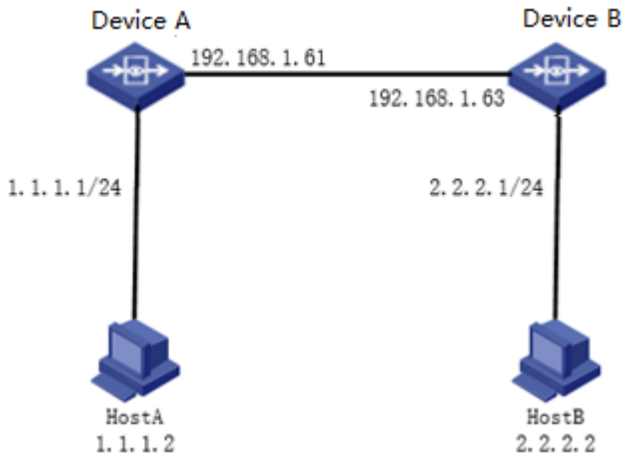
1.5 国密IPSec典型配置举例

1.5.1 组网需求

如下图 1-24 所示，在设备 A 和设备 B 之间使用国密标准建立一个安全隧道，对 Host A 代表的子网（1.1.1.0/24）与 Host B 代表的子网（2.2.2.0/24）之间的数据流进行安全保护。

1.5.2 组网图

图1-24 IPsec 举例组网图

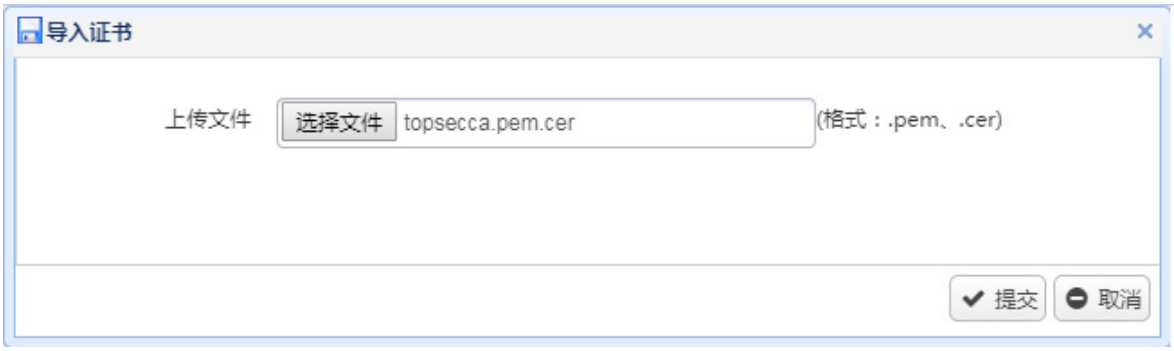


1.5.3 配置步骤

(1) 导入国密 CA 证书

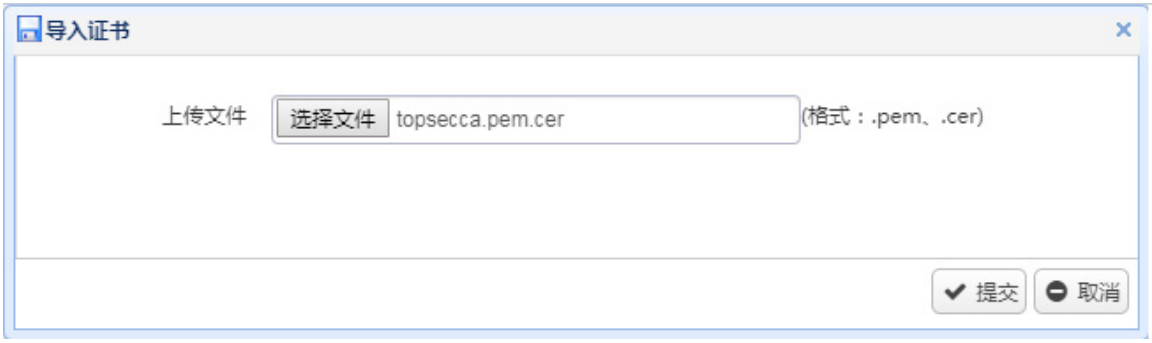
设备 A：进入“策略配置>对象管理>本地证书>证书>CA”，点击导入，如图 1-25 所示。

图1-25 设备 A 导入 CA 证书



设备 B：进入“策略配置>对象管理>本地证书>证书>CA”，点击导入，如图 1-26 所示。

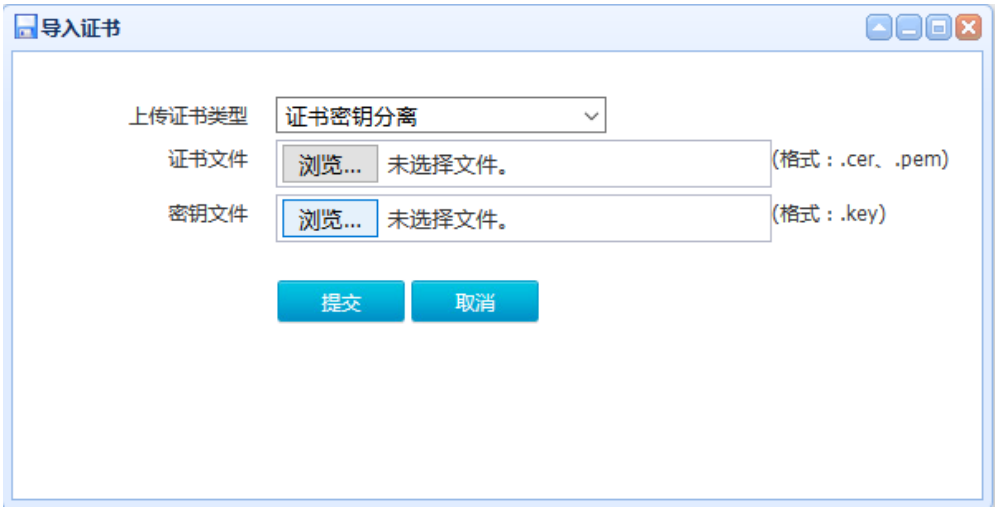
图1-26 设备 B 导入 CA 证书



(2) 导入国密用户证书

设备 A：进入“策略配置>对象管理>本地证书>证书>国密”，点击导入，如图 1-27 所示。上传证书类型选择证书密钥分离。

图1-27 导入国密用户证书



设备 B：进入“策略配置>对象管理>本地证书>证书>国密”，点击导入，上传证书类型选择证书密钥分离。

(3) 新建 IKE 协商

对设备 A 的 IKE 配置如下图 1-28 所示。

图1-28 设备 A 的 IKE 配置

注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

对设备 B 的 IKE 配置如下图 1-29 所示。

图1-29 设备 B 的 IKE 配置

注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

(4) 配置 IPsec 协商策略

对设备 A 的 IPsec 协商策略配置如下图 1-30 所示。

图1-30 设备 A 的 IPsec 协商策略配置

对设备 B 的 IPsec 协商策略配置如下图 1-31 所示。

图1-31 设备 B 的 IPsec 协商策略配置

(5) 新建所需地址对象

图1-32 设备 地址对象配置

		名称	内容(网络，范围，主机，域名)	排除地址	描述	引用	操作
4		ChinaTelecom	1.0.1.0/24, 1.0.2.0/23, 1.0.8.0/21, 1.0.32.0/19, 1.1.0.0/24, ...		中国电信	0	
5		ChinaEducation	1.51.0.0/20, 1.51.16.0/20, 1.51.32.0/19, 1.51.64.0/19, 1.51.96.0/20, ...		中国教育网	1	
6		ChinaMobile	36.128.0.0/12, 36.144.0.0/14, 36.148.0.0/16, 36.149.0.0/16, 36.150.0.0/15, ...		中国移动	0	
7		1_24	1.1.1.0/24			0	
8		2_24	2.2.2.0/24			0	

(6) 新建 IPSec 安全策略

图1-33 设备 A 的配置信息

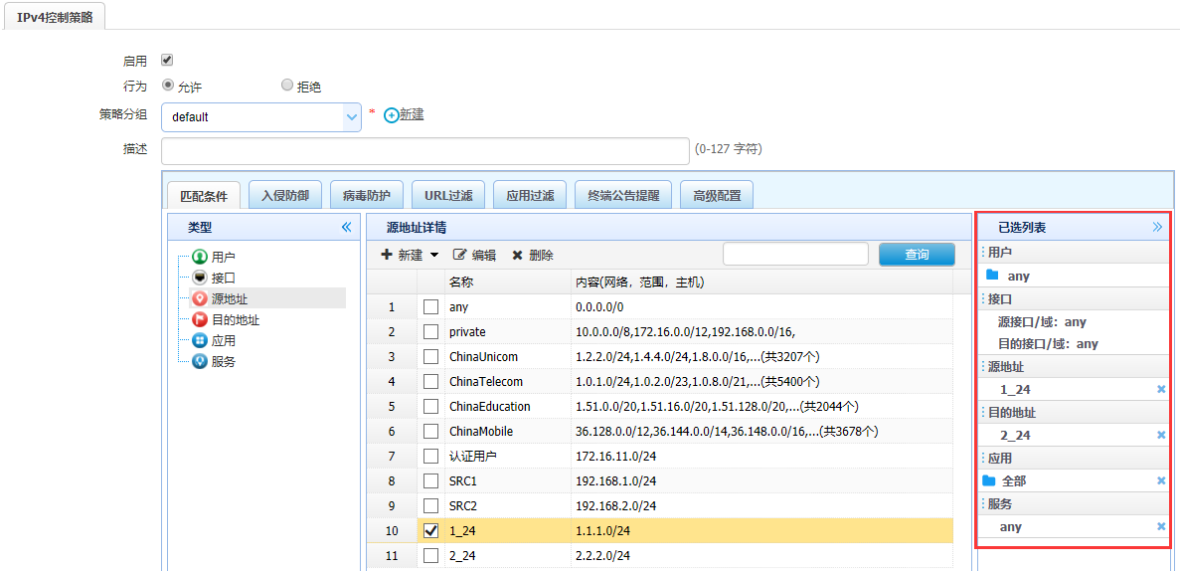
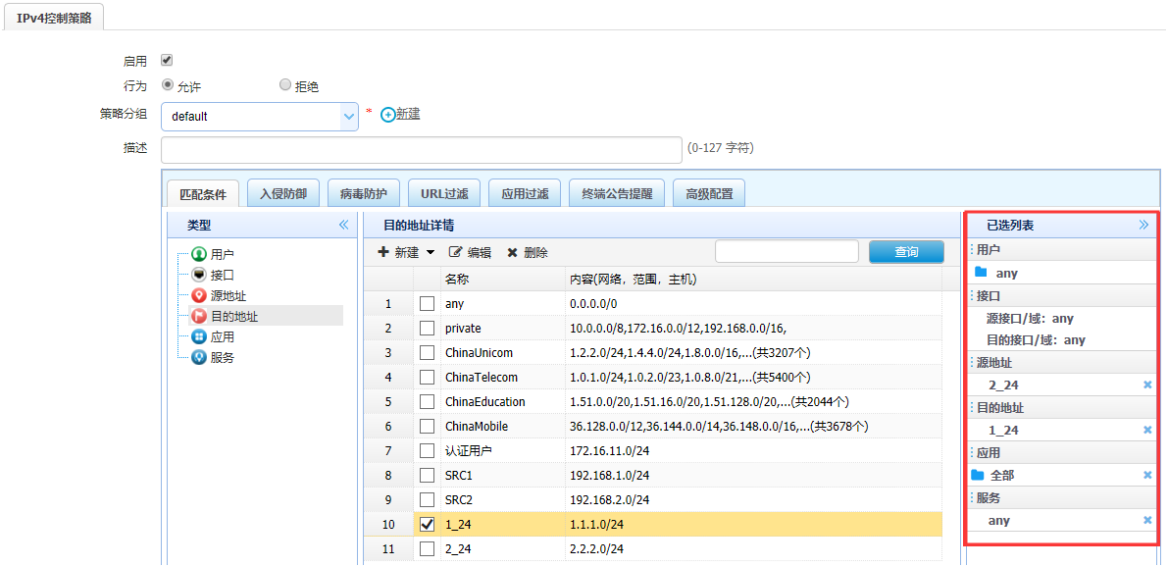


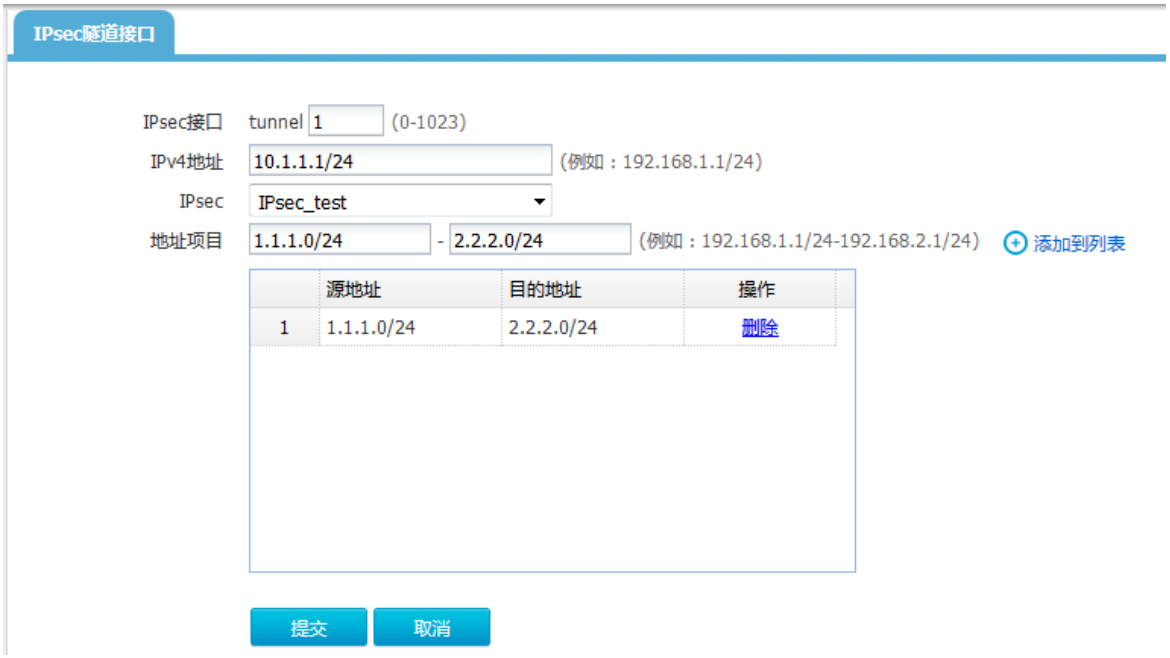
图1-34 设备 B 的配置信息



(7) 新建 IPSEC 隧道接口

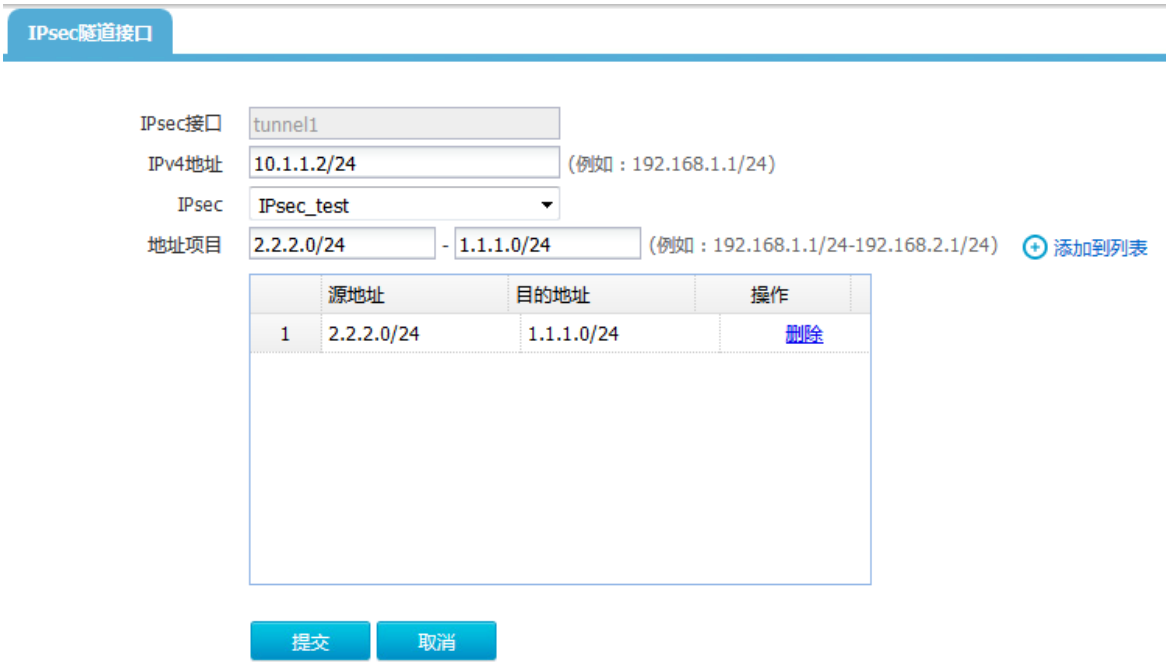
设备 A 的隧道接口如图 1-35 下所示。

图1-35 设备 A 的隧道接口配置



设备 B 的隧道接口如下图 1-36 所示。

图1-36 设备 B 的隧道接口配置



注：配置 IPsec 隧道时，隧道接口地址可选配置。是否配置隧道地址与怎样配置静态路由有关。配置隧道地址后路由可指定下一跳地址的方式去写。未配置隧道地址时需选用出接口的方式去写路由。

(8) 配置静态路由

需要将感兴趣流的路由指向 tunnel 口。

图1-37 设备 A 静态路由配置

出接口配置方式：

下一跳配置方式：

图1-38 设备 B 静态路由配置

出接口配置方式：

下一跳配置方式：

1.5.4 验证配置结果

在导航栏中选择“网络配置 > VPN > IPsec-VPN > IPsec 第三方对接> IPsec SA”，查看 IPsec SA。

图1-39 设备 A 的 IPsec SA

		名称	对端网关	本地网关	状态	过期时间/过期流	流量(入/出)	源网络	目的网络	操作
1	☐	IPsec_test	192.168.1.63	192.168.1.61	连接	0s/0.0KB	0.00kb/0.00kb	1.1.1.0/24	2.2.2.0/24	

图1-40 设备 B 的 IPsec SA

		名称	对端网关	本地网关	状态	过期时间/过期流	流量(入/出)	源网络	目的网络	操作
1	☐	IPsec_test	192.168.1.61	192.168.1.63	连接	0s/0.0KB	0.00kb/0.00kb	2.2.2.0/24	1.1.1.0/24	

2 IPsec 快速配置

2.1 IPsec快速配置概述

由于连锁酒店分支机构众多，IPSEC VPN 业务的部署和维护非常复杂，给管理员的工作带来非常大的挑战：“VPN 业务多变，管理复杂”，现有标准 IPSEC VPN 的配置比较繁琐，组网变化带来的配置改动比较大。因此急需提供一种易用性更好，配置更简洁的解决方案。IPSEC 快速配置就是在这样的场景下应运而生的。

按照以往 VPN 的配置，一个分支上线会有很多相关配置，步骤较多，且在隧道显示上也不太友好，主要表现在如下几个方面：

- 每个分支上线都需要创建 IKE、IPsec 和对应的 tunnel 口，然后在 tunnel 口配置感兴趣流，和对应的 tunnel 路由。中心端有多少个 IP，分支端就需要创建多少个 IKE、IPsec 和 tunnel 口及 tunnel 路由。当走 IPsec 隧道的网段发生变化时，我们需要同步修改对应的感兴趣流和 tunnel 路由。当分支特别多的时候，对于管理员来说是一项非常巨大且繁琐的工作，很容易出现配置错误，不好排查。
- 在 web 页面查看各隧道的流量和状态时，每个隧道只能显示本端 IP 和对端 IP，却不知道这条隧道对应的哪个分支，需要根据分支和 IP 的对应关系，才能知道属于哪个分支。且一个分支的多个感兴趣流会显示多个 SA，无法聚合，显得比较杂乱，不便查看。
- 如果一个分支的私有网段和另一个分支的私有网段有冲突，如，都使用了 192.168.10.1/24 网段，则后上线的分支需要做 NAT，转换为另外一个不冲突的网段才能正常工作。这个 NAT 配置需要绑定对应的隧道口，以明确只有过隧道的流量才需要转换。如果隧道口有变动，则相应的 NAT 配置也需要做对应变动。

鉴于以上配置上的繁琐和显示上的不友好，我们要做出改进，优化连锁酒店的 IPSEC VPN 管理工作，尽可能地使 VPN 配置自动化，简单化，甚至是傻瓜化，做到“快速上线、动态适应、部署简单”。

针对以上目标，IPSEC 快速配置具体的改进措施如下：

- 隐藏 IKE/IPsec/tunnel 口的创建过程
- 管理员只需配置本端分支名称，对端 IP 和预共享密钥。后台根据这些配置，自动生成对应的 IKE、IPsec 和 tunnel 口，其它相关参数均使用内置的默认参数。
- 感兴趣流不再配置，tunnel 路由不再配置
- 管理员只需要配置本端的保护网段，即需要走 IPsec 的源网段。对端也是如此。当两端建立起 IKE 后，交互各自的保护网段，形成感兴趣流，同时以对端的保护网段为目的网段，生成对应的 tunnel 路由。
- 支持多线路备份
- 高优先级线路断开后，无缝切换到低优先级的线路；当高优先级线路恢复后，再切换回高优先级线路。
- NAT 规则不再配置
- 管理员只需要配置哪些源网段转换为哪些目的网段。后台会自动生成对应的 NAT 规则。
- 隧道状态展示优化

- 页面显示隧道状态时，以分支名称为 key，一条记录聚合显示该分支相关隧道的信息，便于查看，支持搜索。

2.2 创建IPsec快速配置

2.2.1 配置概述

IPsec 配置的推荐步骤如下表所示。

表2-1 IPsec 快速配置的推荐步骤

配置任务	说明	详细配置
节点基本信息配置	必选	2.2.2
保护网段配置	必选	2.2.3
高级选项配置（选路策略、网段映射）	可选	2.2.4

2.2.2 节点基本信息配置

在导航栏中选择“网络配置>VPN>IPsec-VPN>IPsec 快速配置”，进入 IPsec 快速配置的显示页面，如图 2-1、图 2-2、图 2-3 所示。

图2-1 IPsec 快速配置分支节点显示页面

图2-2 IPsec 快速配置新建对端网关显示页面

图2-3 IPsec 快速配置中心节点显示页

页面的详细说明如表 2-2。

表2-2 IPsec 快速配置显示页面的详细说明

项目	说明
名称	节点的IPSEC名称，多隧道时聚合隧道的名称显示成该名称
节点位置	包含分支节点、中心节点两种类型
新建对端网关	分支对端中心节点IP配置，多隧道时配置多个IP，IP最多配置4个，每配置一个IP就会自动生成一套IKE、IPSEC、tunnel的配置

项目	说明
本端IP配置	中心节点与分支对接的接口IP配置，多个接口配置多个IP，最多配置4个IP，每配置一个IP就会自动生成一套IKE、IPSEC、tunnel的配置
预共享密钥	用于分支和中心之间验证对端身份（长度为6-39个字符）

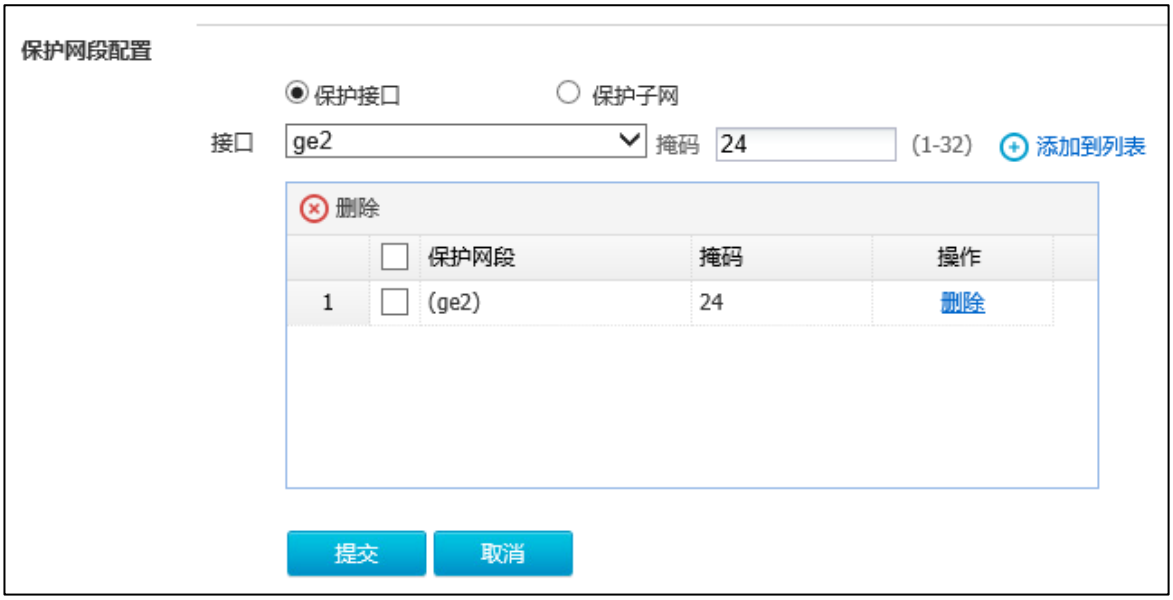
2.2.3 保护网段配置

在导航栏中选择“网络配置 > VPN > IPsec-VPN > IPsec 快速配置”，进入 IPsec 保护网段的显示页面，单击<保护接口>按钮，在接口列表中选择<接口 >并设置掩码，或者单击<保护子网>按钮，设置保护网段和掩码，如图 2-4 所示。

图2-4 IPsec 保护子网配置页面

点击左侧<保护接口>按钮可以保护接口配置选项，如图 2-5 所示。

图2-5 IPsec 协商策略详细配置页面



页面的详细说明如表 2-3 所示。

表2-3 IPsec 保护网段配置的详细说明

项目	说明
保护接口	自动根据保护接口IP及掩码生成保护网段，该网段会自动传递给对端网关，对端网关根据此保护网段自动生成相应tunnel口的路由。
保护子网	该网段会自动传递给对端网关，对端网关根据此保护网段自动生成相应tunnel口的路由。

输入完毕后，点击<添加到列表>，点击<提交>按钮，应用配置。

在 IPsec 保护网段列表中，点击保护网段右侧的<删除>按钮，可以删除对应的保护网段，或者选中多个条目，点击左上角的<删除>按钮，批量删除多个保护网段的配置。

2.2.4 高级选项配置

在导航栏中选择“网络配置 > VPN > IPsec-VPN > IPsec 快速配置”，节点类型选择<分支节点>，单击对端网关<新建>按钮，进入分支节点“高级选项配置”。如图 2-6 所示。

图2-6 IPsec 分支节点高级选项选路策略配置页面

输入线路名称、线路 IP，点击<添加到列表>，点击<提交>应用配置。

点击右侧<网段映射>，进入高级选项-网段映射配置页面，如图 2-7 所示。

图2-7 IPsec 分支节点高级选项网段映射配置页面

输入源网段、映射后网段，点击<添加到列表>，点击<提交>应用配置。

页面的详细说明如表 2-4 所示。

表2-4 IPsec 高级选项的详细说明

项目	说明
选路策略	选路策略中的线路顺序决定了不同隧道的路由优先级，规格支持配置4条线路。
线路名称	设置线路名称。
线路IP	设置线路对应的IP，线路IP必须在对端网关IP中。
网段映射	一对一NAT映射，源网段和映射后网段掩码必须一致，按照IP的顺序进行一对一映射，最多支持32个网段映射。
源网段	映射前源网段。
映射后网段	映射后目的网段，在对端网关看到的保护网段是映射后网段。

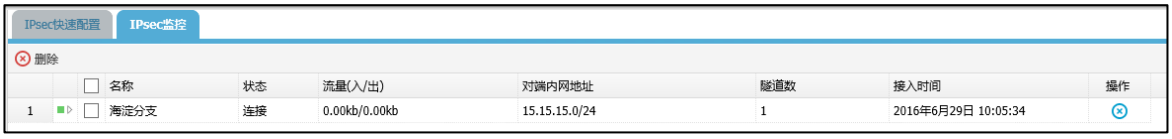
说明：中心节点高线选项配置只有网段映射，没有选路策略，选路策略只需在分支节点配置，分支节点配置的选路策略会自动同步给中心节点。

2.3 IPsec状态监控

2.3.1 查看 IPsec 监控

在导航栏中选择“网络配置 > VPN > IPsec-VPN 快速配置 > IPsec 监控”，进入 IPsec 监控显示页面。页面中显示了已经新建的 IPsec 聚合隧道。如图 2-8 所示。

图2-8 IPsec 监控显示页面



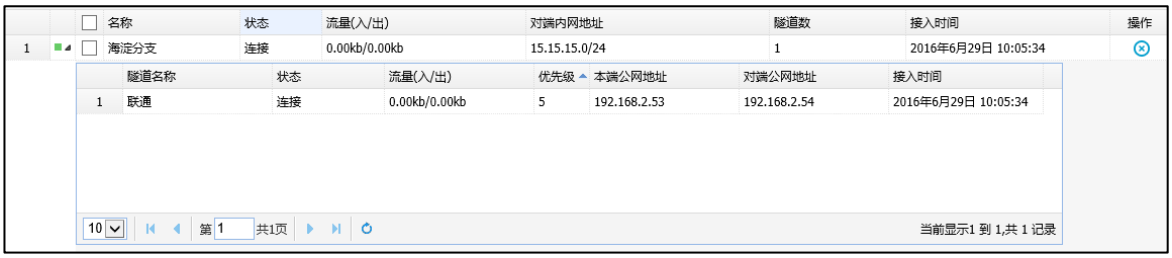
页面的详细说明如表 2-5。

表2-5 IPsec 监控显示页面的详细说明

项目	说明
名称	对端IPSEC名称。
状态	IPSEC SA状态。
流量（入/出）	聚合隧道的双向总流量。
对端内网地址	对端保护网段。
隧道数	分支与中心设备之间建立的隧道数量计数。
接入时间	隧道建立时间。
操作	点击可删除聚合隧道。

点击聚合隧道左侧的 按钮，可以展开显示各隧道的详细情况，如图 2-9 所示。

图2-9



页面的详细说明如表 2-6。

表2-6 IPsec 监控显示页面的详细说明

项目	说明
隧道名称	隧道名称，显示为分支端配置的选路策略中的线路名称。
状态	隧道IPSEC SA状态。
流量（入/出）	隧道的双向流量统计。
优先级	隧道优先级，多隧道备份时流量优先走优先级数值小的隧道，其它隧道做备份。
隧道数	分支与中心设备之间建立的隧道数量计数。
本端公网地址	隧道本端的公网地址。
对端公网地址	隧道对端的公网地址。
接入时间	隧道建立时间。

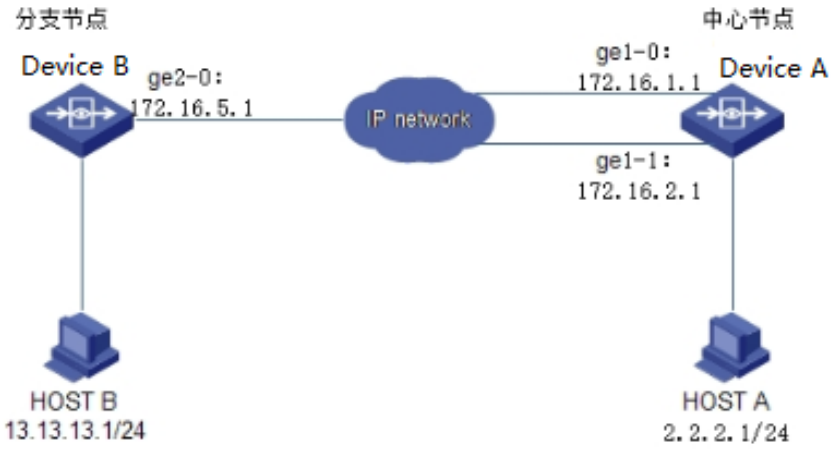
2.4 IPSec典型配置举例

2.4.1 组网需求

如下图 2-10 所示，在设备 A 和设备 B 之间建立两个安全隧道，对 Host A 代表的子网（2.2.2.0/24）与 Host B 代表的子网（13.13.13.0/24）之间的数据流进行安全保护，同时实现隧道备份。

2.4.2 组网图

图2-10 IPsec 举例组网图



2.4.3 配置步骤

(1) 中心设备 IPSEC 快速配置

对设备 A 的 IPSEC 配置如图 2-11 所示。

图2-11 设备 A 的 IPSEC 快速配置

(2) 分支设备 IPSEC 快速配置

对设备 B 的 IPSEC 快速配置如图 2-12、图 2-13 所示。

图2-12 设备 B 的 ISPEC 快速配置

图2-13 设备 B 选路策略配置

2.4.4 验证配置结果

在导航栏中选择“网络配置 > VPN > IPsec-VPN >IPsec 快速配置> IPsec 监控”，查看隧道建立状态。

图2-14 设备 A 的 IPsec 监控

图2-15 设备 B 的 IPsec 监控

目 录

1 VPN 链路备份 ····· 1-1
1.1 概述 ····· 1-1
1.2 VPN 链路备份配置 ····· 1-1
1.2.1 配置 IPsec 主链路 ····· 1-1
1.2.2 配置 IPsec 备链路 ····· 1-2
1.2.3 配置 IPsec 隧道接口 ····· 1-3
1.3 IPsec 链路备份配置举例 ····· 1-4

1 VPN 链路备份

1.1 概述

为了保障 VPN 链路的稳定性和可用性，可以在设备上配置一主一备 2 条 IPSec VPN 链路，在一条 IPSec VPN 链路不通的情况下，即一段时间无法建立链接时，启用另一条 IPSec VPN 链路。

1.2 VPN链路备份配置

1.2.1 配置 IPsec 主链路

在导航栏中选择“网络配置 > VPN > IPsec-VPN>IPsec 第三方对接”，参照 IPSEC 配置，新建一条 IKE 后，选择该条目再选择新建一条 ipsec，进入主链路配置页面，如图 1-1 所示。

图1-1 主链路配置页面

表1-1 主链路配置详细说明

项目	说明
密钥周期	指定IPSEC SA最大有效时间，有时间、流量、时间+流量三种选择。
秒	IPSEC SA最大有效时间。
连接方式	连接方式，可选择自动连接、流量触发连接、监控链路故障自动连接。
时间	自动连接时间。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

1.2.2 配置 IPsec 备链路

在导航栏中选择“网络配置 > VPN > IPsec-VPN>Ipsec 第三方对接”，参照 IPSEC 配置，新建一条 IKE 后，选择该条目再选择新建一条 ipsec，进入备链路配置页面，如图 1-2 所示。

图1-2 备链路配置页面

页面的相关配置的详细说明如表 1-2 所示（其余参数说明参见 IPsec 相关配置）。

表1-2 备链路配置详细说明

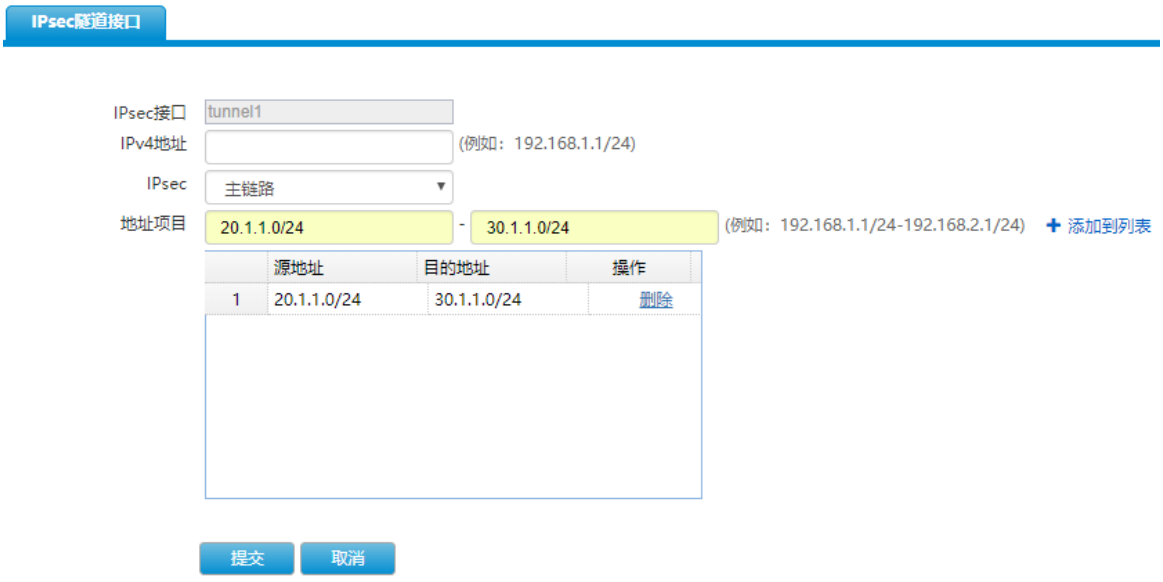
项目	说明
密钥周期	指定IPSEC SA最大有效时间，有时间、流量、时间+流量三种选择。
秒	IPSEC SA最大有效时间。
连接方式	连接方式，可选择自动连接、流量触发连接、监控链路故障自动连接。
时间	自动连接时间。
主链路	选择作为该备份链路的主链路。
切换延迟时间	主备链路切换时间。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

1.2.3 配置 IPsec 隧道接口

在导航栏中选择“网络配置 > VPN > IPsec-VPN > IPsec 第三方对接 > IPsec 隧道接口”，进入 IPsec 隧道接口的显示页面，如图 1-3 所示。

图1-3 配置 IPsec 隧道接口



点击<提交>后，可以查看 IPsec 隧道。

图1-4 查看 IPsec 隧道

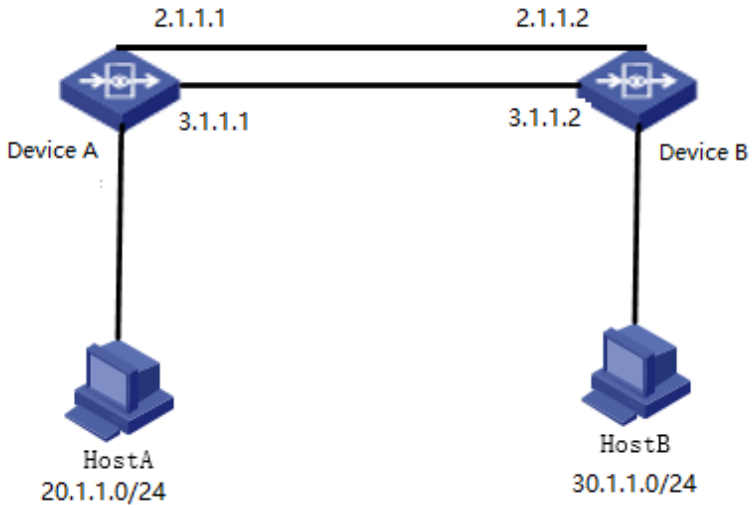
1.3 IPsec链路备份配置举例

1. 组网需求

主链路断开后，备链路自动连接，主链路重新连接后，备链路自动断开。

2. 组网图

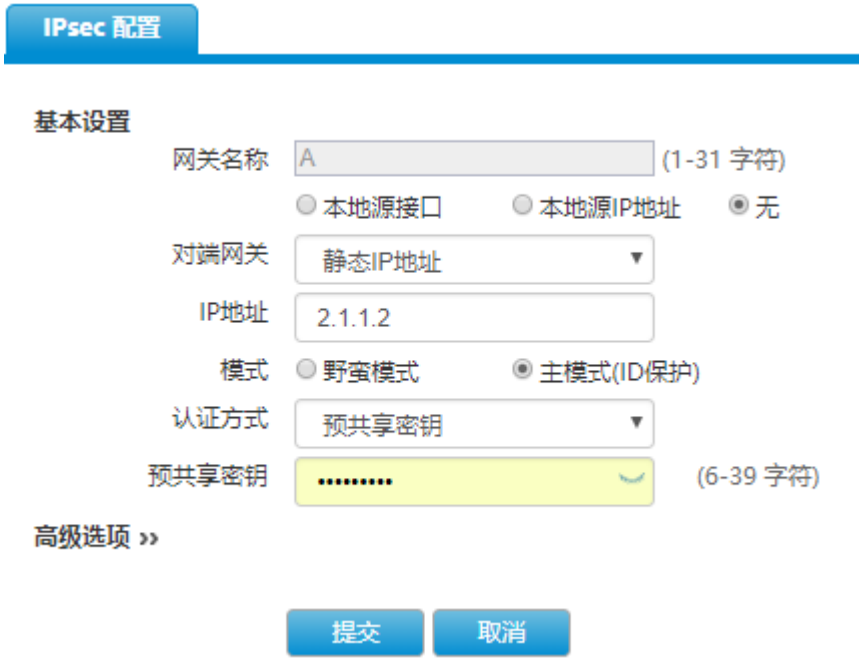
图1-5 组网图



3. 配置步骤

(1) 新建设备 A 的 ike。

图1-6 新建设备 A 的主链路 ike



(2) 新建设备 A 的主链路 ipsec

图1-7 新建设备 A 的 ipsec

(3)　新建设备 A 的备链路的 ike。

图1-8 新建设备 A 的备链路的 ike

(4)　新建设备 A 的备链路的 ipsec。

图1-9 新建设备 A 的备链路的 ipsec

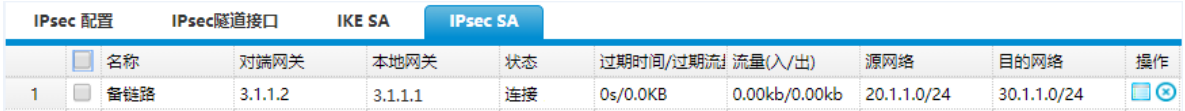
(5) 新建设备 A 的主备链路 ipsec 隧道接口。

图1-10 主备链路 ipsec 隧道接口

(6) 设备 B 照上述步骤重复。

(7) 验证主链路断开时备份链路自动连接。

图1-11 备链路连接



(8) 验证主链路恢复后，备链路断开连接。

图1-12 主链路恢复连接

目 录

1 SSL VPN ····· 1-1

1.1 SSL VPN 概述 ····· 1-1

1.2 使用限制 ····· 1-1

1.3 配置 SSL VPN ····· 1-1

1.3.1 配置概述 ····· 1-1

1.3.2 配置 SSL VPN 资源 ····· 1-2

1.3.3 配置 SSL VPN 门户网站 ····· 1-3

1.3.4 配置 SSL VPN 策略 ····· 1-4

1.3.5 配置 SSL VPN 全局配置 ····· 1-6

1.3.6 配置 SSL VPN IP 用户绑定 ····· 1-8

1.3.7 配置 SSL VPN 安全设置 ····· 1-9

1.4 SSL VPN 的查看和管理 ····· 1-10

1.4.1 在线用户 ····· 1-10

1.5 SSL VPN 典型配置举例 ····· 1-11

1.5.1 组网需求 ····· 1-11

1.5.2 配置思路 ····· 1-12

1.5.3 配置步骤 ····· 1-12

1.5.4 验证配置 ····· 1-17

1.6 SSL VPN 客户端的安装及配置 ····· 1-18

1.6.1 SSL VPN 客户端安装软件的获取 ····· 1-18

1.6.2 Windows 系统 SSL VPN 客户端安装及配置 ····· 1-18

1.6.3 Android 系统 SSL VPN 客户端安装及配置 ····· 1-25

1 SSL VPN

1.1 SSL VPN概述

SSL VPN 以 SSL（Secure Sockets Layer，安全套接字层）为基础提供远程的安全连接服务。用户可通过互联网，使用内嵌 SSL 协议的浏览器与远端的 Web 服务器建立安全的连接，访问内部资源。企业或机构可通过 SSL VPN 来为移动用户或者外部客户提供访问内部资源的服务并保证安全性。

SSL VPN 服务通过 SSL VPN 网关来提供。SSL VPN 网关位于远端接入用户和企业内部网络之间，负责在二者之间转发报文。管理员需要在 SSL VPN 网关上创建与企业网内服务器对应的资源。

SSL VPN 网关与远端接入用户建立 SSL 连接，并对接入用户进行身份认证。远端接入用户的访问请求只有通过 SSL VPN 网关的安全检查和认证后，才会被 SSL VPN 网关转发到企业网络内部，从而实现对企业内部资源的保护。

1.2 使用限制

(1) SSL VPN 客户端需使用与设备版本配套的客户端软件，客户端软件随版本一起发布，您可以登录 www.h3c.com 官网，在版本下载处下载安装使用。

(2) SSL VPN 功能支持 Windows7 和 Windows10 操作系统，以及 Android6.0 以上的移动端，暂不支持苹果 iOS、Mac OS 系统和 Linux 操作系统。

(3) SSL VPN 默认支持接入用户数为 10 个，不支持数量扩充。

1.3 配置SSL VPN

1.3.1 配置概述

SSL VPN 配置的推荐步骤如表 1-1 所示。

表1-1 IPsec 配置的推荐步骤

配置任务	说明	详细配置
配置用户/用户组	必选	详见“用户和用户认证”章节
配置SSL VPN资源	必选	1.3.2
配置SSL VPN门户网站	可选	1.3.3
配置SSL VPN策略	必选	1.3.4
配置SSL VPN 全局配置	必选	1.3.5
配置SSL VPN IP用户绑定	可选	1.3.7
配置SSL VPN安全设置	可选	1.3.7

1.3.2 配置 SSL VPN 资源

在导航栏中选择“网络配置 > VPN > SSL VPN > 资源”，进入 SSL VPN 资源配置的显示页面，单击<新建>按钮，或者点击对应资源的右侧<编辑>按钮，进入资源的配置页面，如图 1-1 所示。

图1-1 资源新建页面

页面的详细说明如表 1-2 所示。

表1-2 资源配置的详细说明

项目	说明
名称	资源策略名称。
描述	资源策略的描述。
资源地址	授权资源的IP地址，最多支持32组。
资源类型	授权资源的类型，可选择：any、http、https、ftp、icmp、ssh、telnet、邮件、自定义tcp端口和自定义udp端口。

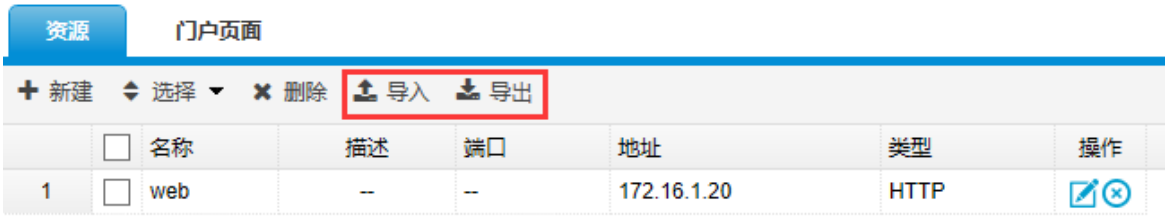
输入完毕后，点击<提交>按钮，应用配置。

在资源显示页面，点击对应资源的<删除>按钮，可以删除对应的资源，如图 1-2 所示。

图1-2 资源删除

在资源显示页面，点击<导入><导出>按钮，可以将所有的资源导出成 csv 文件。点击<导入>按钮可以将导出的 csv 文件中的资源导入到系统中，如图 1-3 所示。

图1-3 资源导入/导出



1.3.3 配置 SSL VPN 门户网站

在导航栏中选择“网络配置 > VPN > SSL VPN > 资源”，选择门户网站页签，进入门户网站的配置页面，如图 1-4 所示。

图1-4 门户网站配置页面

页面的详细说明如表 1-3 所示。

表1-3 门户网站配置的详细说明

项目	说明
页面标题	网站标题。
网页logo	网站标题的logo。
公告	网站的公告内容。
客户端下载	填写VPN客户端下载地址。

输入完毕后，点击<提交>按钮，应用配置。

1.3.4 配置 SSL VPN 策略

在导航栏中选择“网络配置 > VPN > SSL VPN > 策略”，进入策略配置的显示页面，单击<新建>按钮，或者点击对应 SSL VPN 策略的右侧<编辑>按钮，进入 SSL VPN 策略的配置页面，如图 1-5 所示。

图1-5 SSL VPN 策略页面

页面的详细说明如表 1-4 所示。

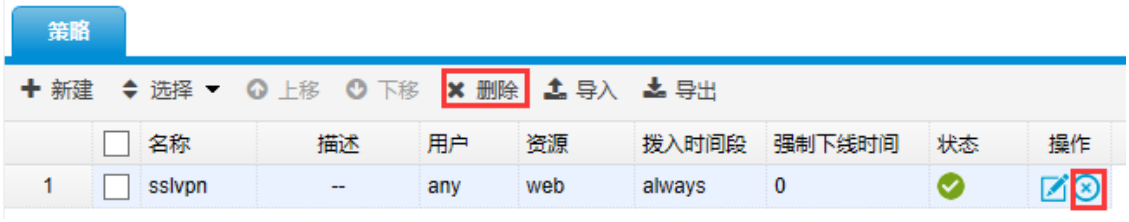
表1-4 SSL VPN 策略配置的详细说明

项目	说明
启用	SSL VPN启用/禁用开关。
名称	SSL VPN策略名称。
描述	SSL VPN策略描述。
用户	SSL VPN授权登录用户。
授权资源	SSL VPN授权资源。
拨入时间段	SSL VPN授权拨入时间段。
强制下线时间	SSL VPN用户强制下线时间。

输入完毕后，点击<提交>按钮，应用配置。

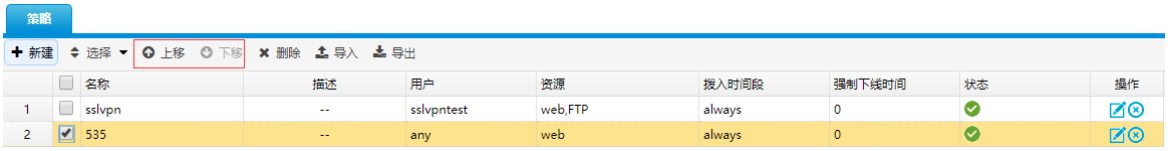
在策略显示页面，点击对应策略的<删除>按钮，可以删除对应的策略。如图 1-6 所示。

图1-6 策略删除



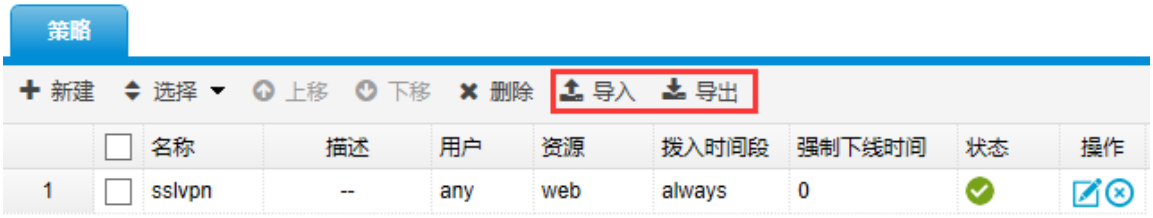
在资源策略显示页面，点击<上移>、<下移>按钮，可以调整策略的优先级。如图 1-7 所示。

图1-7 策略优先级调整



在策略显示页面，点击<导入><导出>按钮，可以将所有的策略导出成 csv 文件。点击<导入>按钮可以将导出的 csv 文件中的策略导入到系统中。如图 1-8 所示。

图1-8 策略导入/导出



1.3.5 配置 SSL VPN 全局配置

在导航栏中选择“网络配置 > VPN > SSL VPN > 全局配置”，进入全局配置的配置页面。如图 1-9 所示。

图1-9 全局配置页面

页面的详细说明如表 1-5。

表1-5 SSL VPN 全局配置的详细说明

项目	说明
启用	全局配置启用/禁用开关
拨入接口	SSL VPN客户端拨入IP地址所在接口。
SSL VPN端口	SSL VPN客户端拨入端口号。SSL VPN使用UDP协议进行通信，端口号为UDP端口，默认为1194，可配置为1024-65534之间未被系统使用的端口。
全局DNS设置	SSL VPN客户端拨入成功，客户端获取到的DNS地址。
地址池	SSL VPN客户端拨入成功，客户端分配到的IP地址。

项目	说明
子网路由	SSL VPN客户端拨入成功，客户端允许访问的地址。
允许多处登录	勾选后，可支持同一个SSL VPN用户在多地同时登录。
证书登录	勾选后，可支持指定证书进行SSL VPN登录 ● CA证书：引用本地证书>证书>CA证书，支持PEM格式证书 ● 本端证书：引用本地证书>证书>本地证书 ● 对端证书：引用本地证书>证书>本地证书
心跳报文间隔	客户端和设备发送心跳报文间隔
心跳未反馈重连	超过设置心跳未反馈次数后客户端重连

输入完毕后，点击<提交>按钮，应用配置。

1.3.6 配置 SSL VPN IP 用户绑定

在导航栏中选择“网络配置 > VPN > SSL VPN > 全局配置 ”，选择 IP 用户绑定页签，单击<新建>按钮，进入 IP 用户绑定策略的配置页面，如图 1-10 所示。

图1-10 IP 用户绑定配置页面

页面的详细说明如图 1-6。

表1-6 IP 用户绑定配置页面的详细说明

项目	说明
启用	IP用户绑定功能启用/禁用开关。
用户	绑定的用户，单击输入框或后面的<选择用户>，弹出用户组成员选择窗口。
IP	绑定的IP地址。

输入完毕后，点击<提交>按钮，应用配置。

1.3.7 配置 SSL VPN 安全设置

在导航栏中选择“网络配置 > VPN > SSL VPN > 全局配置”，选择安全设置页签，进入安全设置配置页面，如图 1-11 所示。

图1-11 安全设置配置页面

页面的详细说明如表 1-7。

表1-7 安全设置配置页面的详细说明

项目	说明
防暴力破解功能	防暴力破解功能启用/禁用开关。
同名用户登录	同名用户登录启用/禁用开关。
同名用户登录连续出错	同名用户登录连续出错次数设置。
同名用户登录锁定时间	同名用户登录连续出错次数达到阈值后锁定时间设置。
同IP用户登录	同IP用户登录启用/禁用开关。
同IP用户登录连续出错	同一IP，用户登录连续出错次数设置。
同IP用户登录锁定时间	同一IP，用户登录连续出错次数达到阈值后锁定时间设置。

输入完毕后，点击<提交>按钮，应用配置。

1.4 SSL VPN的查看和管理

1.4.1 在线用户

在导航栏中选择“数据中心 > 系统监控 > SSL VPN 在线用户”，进入在线用户显示页面。页面中显示了已经拨入成功的 SSL VPN 用户。如图 1-12 所示。

图1-12 在线用户显示页面

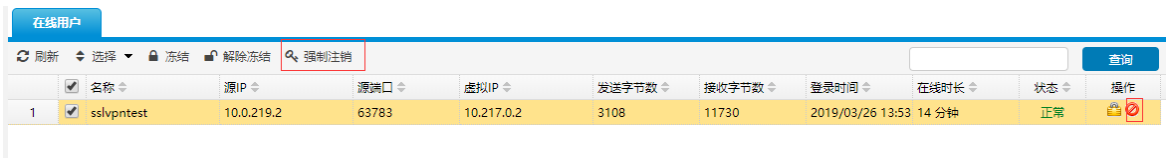
页面的详细说明如表 1-8。

表1-8 在线用户显示页面的详细说明

项目	说明
名称	SSL VPN拨入用户的名称。
源IP	SSL VPN拨入用户的源IP：一般是SSL VPN拨入用户公网出口IP地址
源端口	SSL VPN拨入用户的源端口。
虚拟IP	SSL VPN拨入用户分配到IP地址。
发送字节数	统计SSL VPN拨入用户发送字节数。
接收字节数	统计SSL VPN拨入用户接收字节数。
登录时间	SSL VPN用户登录成功时间。
在线时长	SSL VPN用户拨入后在线时长。
状态	SSL VPN拨入用户状态展示
操作	可以对相应SSL VPN拨入用户进行的操作。

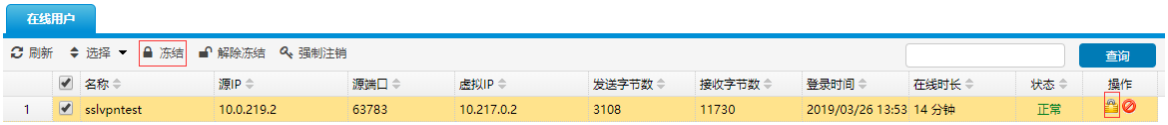
在线用户显示页面，点击<强制注销>按钮，可以将对应在线用户进行注销。如图 1-13 所示

图1-13 在线用户注销



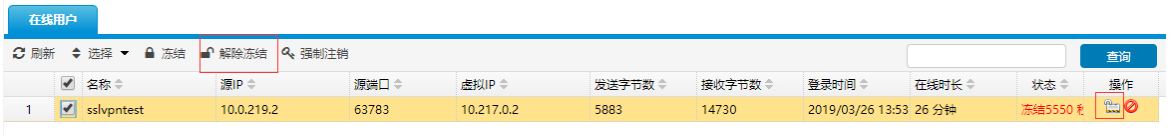
在线用户显示页面，点击<冻结>按钮，可以将对应的在线用户进行冻结。如图 1-14 所示

图1-14 在线用户冻结



在线用户显示页面，点击<解除冻结>按钮，可以将对应的已冻结用户解除冻结。如图 1-15 所示

图1-15 在线用户解除冻结

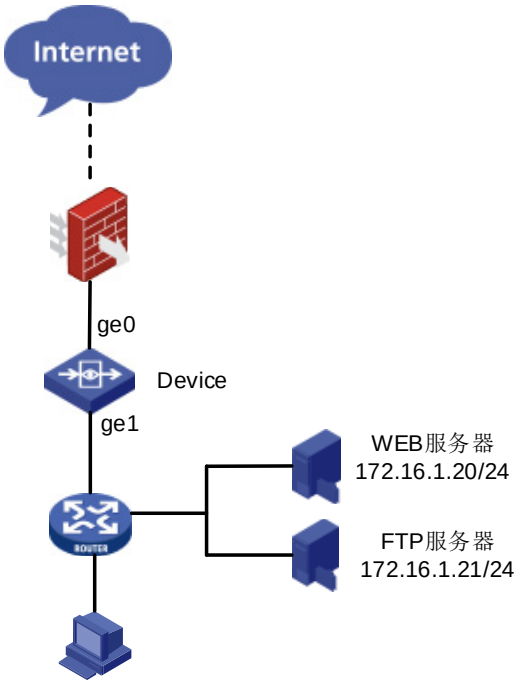


1.5 SSL VPN典型配置举例

1.5.1 组网需求

如图 1-16 所示，使用设备的 ge0 和 ge1 接口以路由方式部署在网络中。用户希望设备提供 SSL VPN 服务，以供互联网用户通过 SSL VPN 访问内网的 Web 和 FTP 服务器。

图1-16 SSL VPN 功能配置组网图



1.5.2 配置思路

(1) 按照组网图组网。

(2) 配置接口。

(3) 配置用户。

(4) 配置 SSL VPN 全局配置。

(5) 配置 SSL VPN 资源。

(6) 配置 SSL VPN 策略

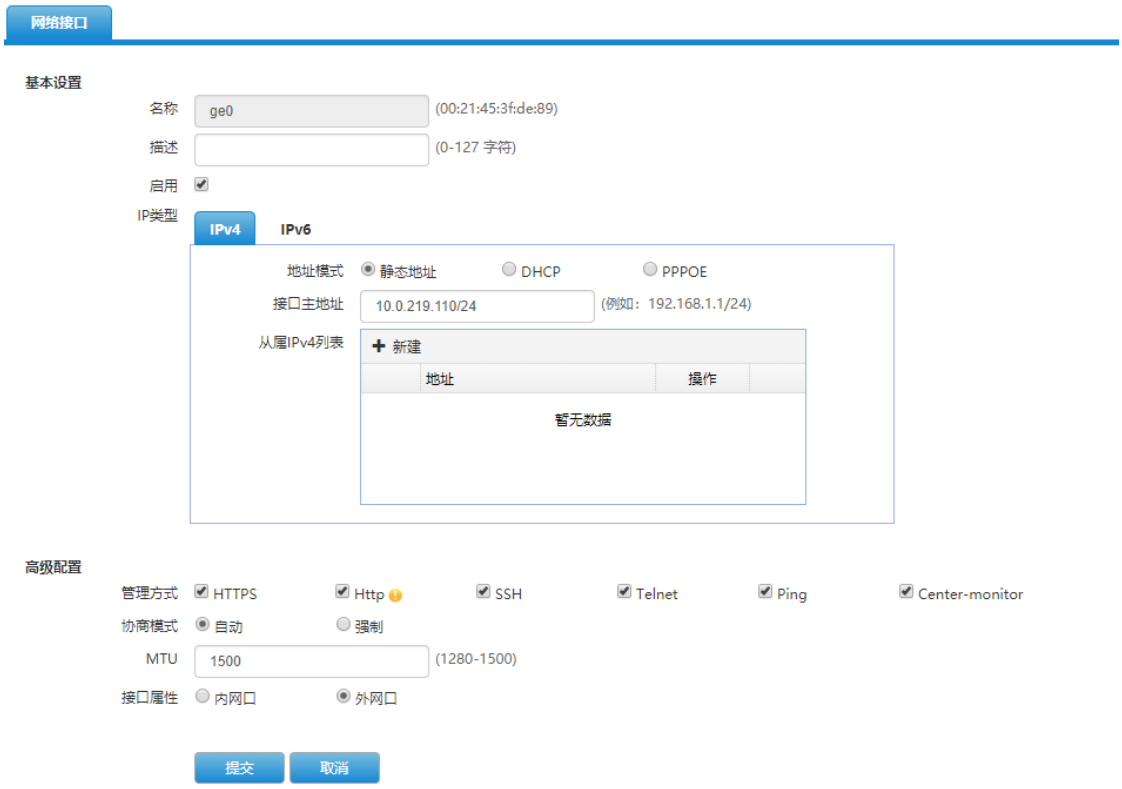
(7) 配置静态路由。

1.5.3 配置步骤

1. 配置接口

如图 1-17 所示，进入“网络配置>接口配置>物理接口”页面，点击“编辑”按钮为 ge0 接口配置 ip 地址，并点击<提交>。

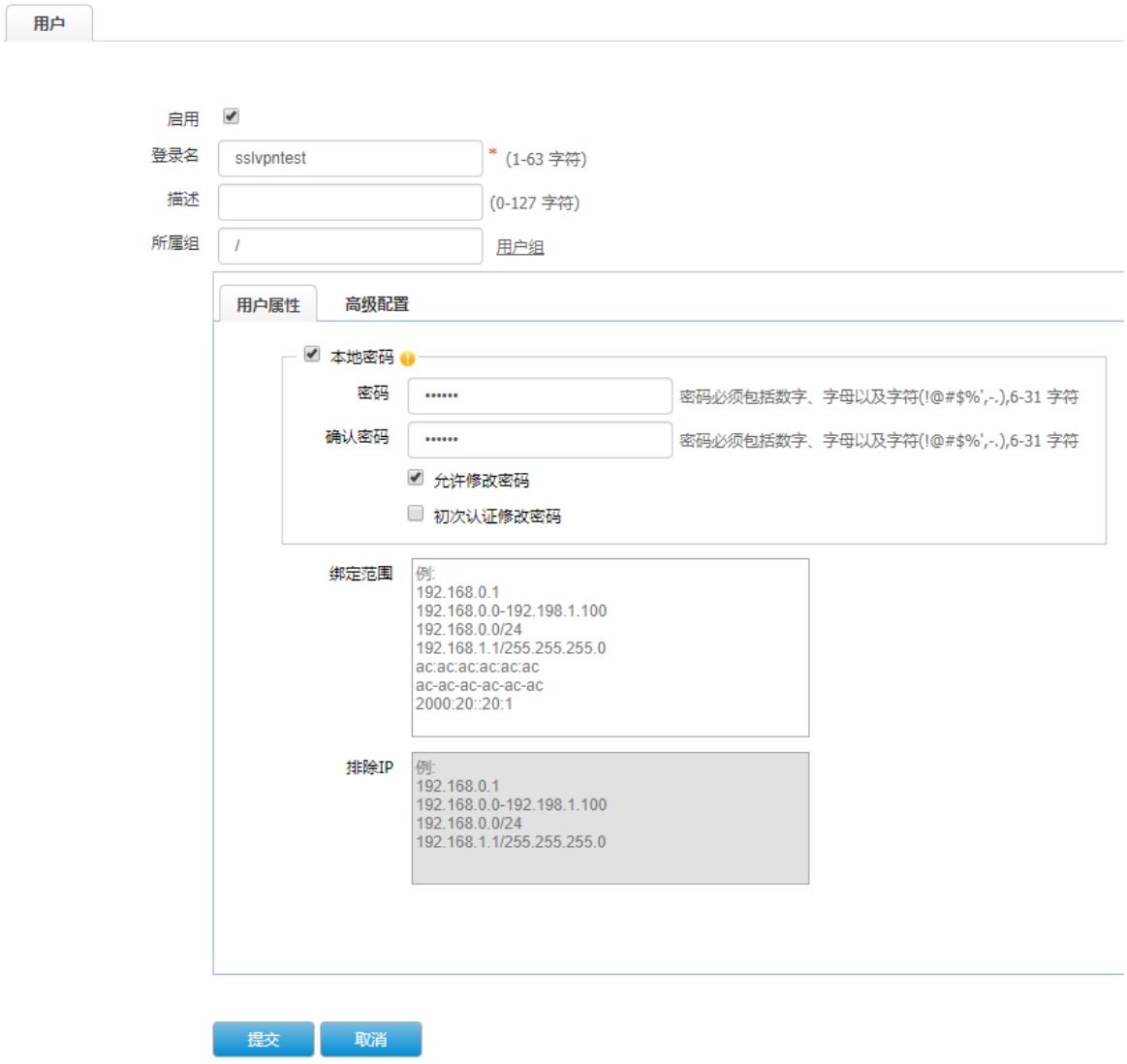
图1-17 配置接口



2. 配置用户

如图 1-18 所示，进入“用户管理> 用户组织结构>用户”页面，点击<新建>按钮，新建用户“sslvpntest”，并点击<提交>。

图1-18 配置用户



3. 配置 SSL VPN 全局配置

如图 1-19 所示，进入“网络配置>VPN> SSL VPN>全局配置”页面，进行 SSL VPN 全局配置，并点击<提交>。

图1-19 配置全局配置

4. 配置 SSL VPN 资源

如图 1-20 和图 1-21 所示，进入“网络配置>VPN> SSL VPN>资源”页面，点击“新建”按钮，进行 SSL VPN 的 web 和 ftp 资源配置，并点击<提交>。

图1-20 配置 HTTP 资源

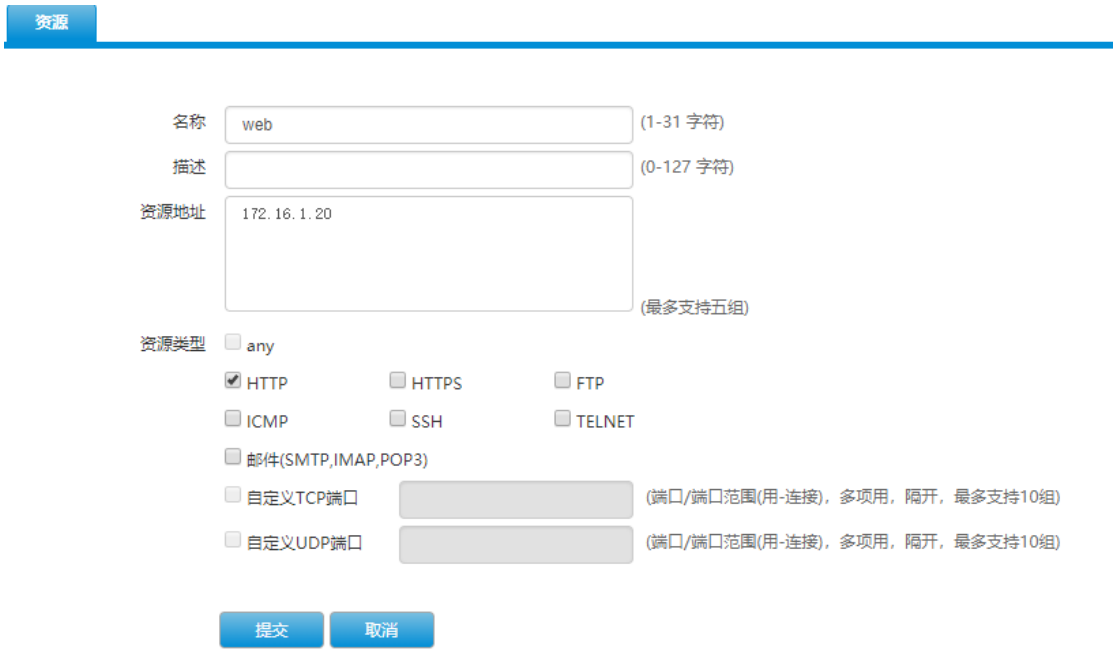


图1-21 配置 ftp 资源

5. 配置 SSL VPN 策略

如图 1-22 所示，进入“网络配置>VPN>SSL VPN>策略”页面，点击<新建>按钮，进行 sslvpn 的策略配置，并点击<提交>。

图1-22 策略配置

6. 配置静态路由

如图 1-23 所示，进入“网络管理>路由>静态路由”页面，点击<新建>按钮，配置一条静态路由：目的网段为服务器的网段：172.16.1.1/24，下一跳为 ge1 对端互联接口地址。

图1-23 配置静态路由

1.5.4 验证配置

(1) 查看 SSL VPN 在线用户

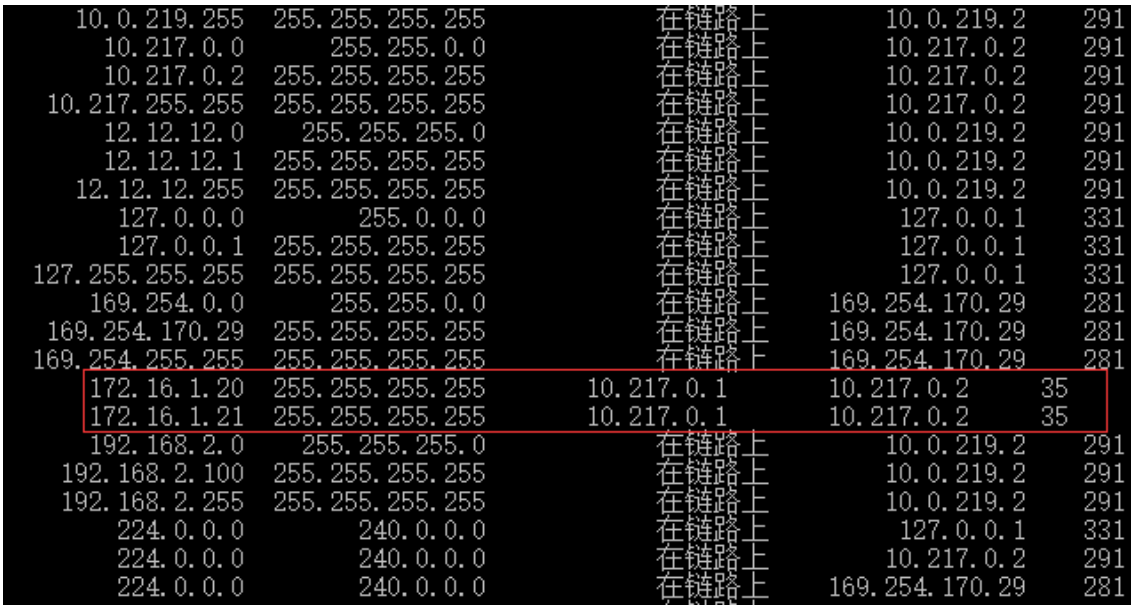
如图 1-24 所示，SSL VPN 连接成功后，进入“数据中心>系统监控>SSL VPN 在线用户”页面，查看在线用户。

图1-24 SSL VPN 在线用户

(2) 查看客户端路由表

如图 1-25 所示，SSL VPN 连接成功后，查看客户端的路由表，下发了两条路由。

图1-25 客户端路由表

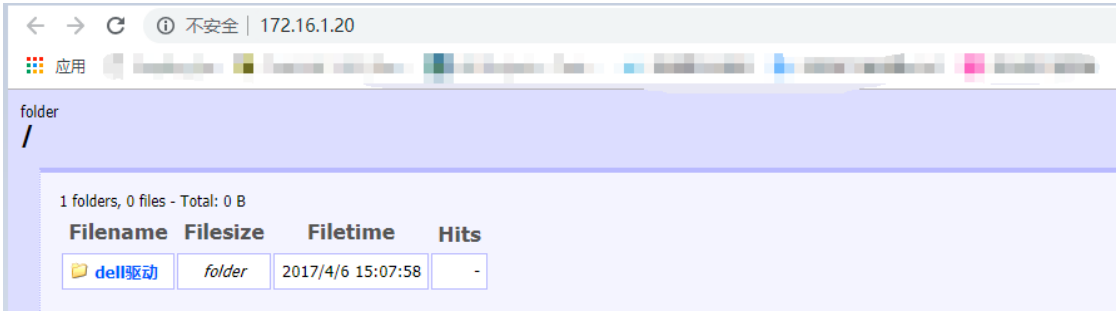


(3) 访问 SSL VPN 资源

SSL VPN 连接成功后，访问内网的 http 和 web 资源，能够访问成功，如图 1-26 和图 1-27 所示。

图1-26 访问 FTP 资源

图1-27 访问 HTTP 资源



1.6 SSL VPN客户端的安装及配置

1.6.1 SSL VPN 客户端安装软件的获取

SSL VPN 客户端需使用与设备版本配套的客户端软件，客户端软件随版本一起发布，您可以登录 www.h3c.com 官网，在版本下载处下载安装使用。

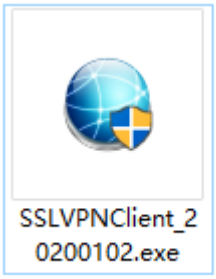
SSL VPN 客户端软件支持 win7 和 win10 操作系统，以及 Android6.0 以上系统，以下分别介绍 Windows 系统和 Android 系统的客户端安装及配置方法。

1.6.2 Windows 系统 SSL VPN 客户端安装及配置

1. 客户端安装

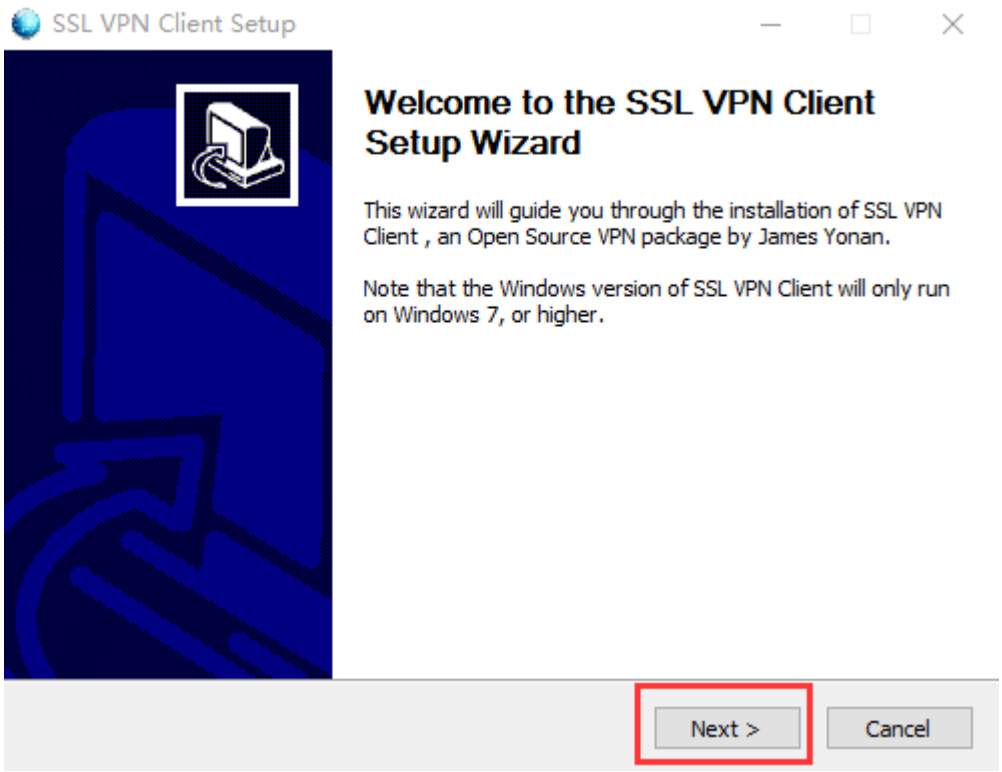
(1) 下载 Windows 系统的 SSL VPN 客户端软件并解压缩，点击运行安装程序，如下图所示。

图1-28 客户端



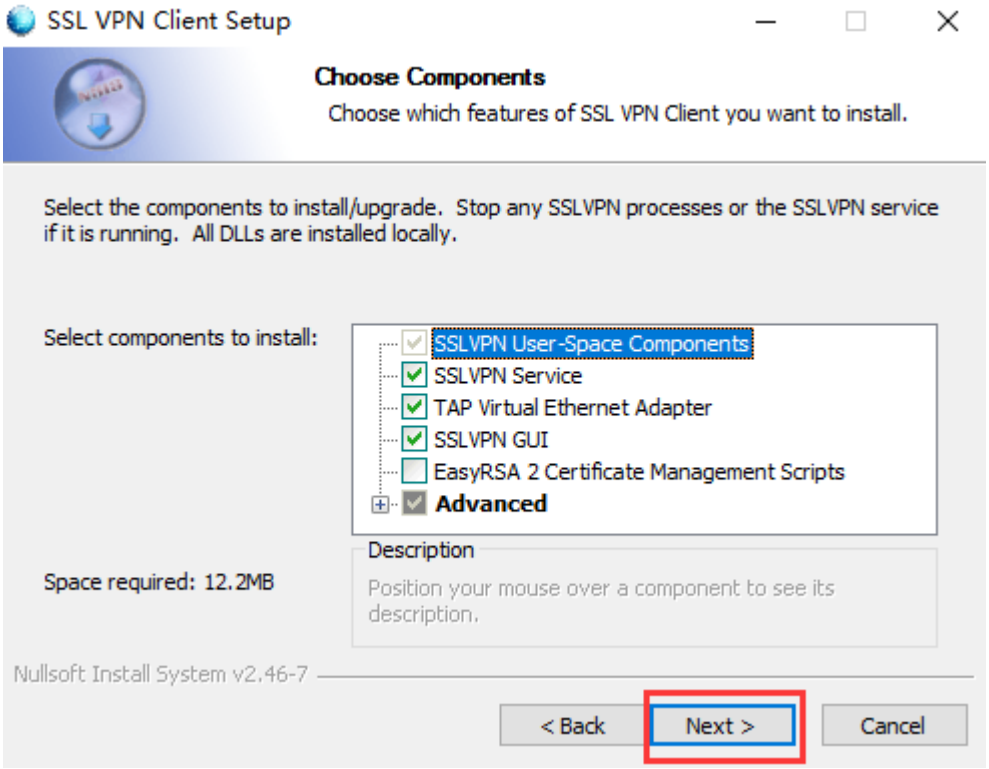
(2) 弹出安装向导页面，点击“Next”进入下一步。

图1-29 开始安装



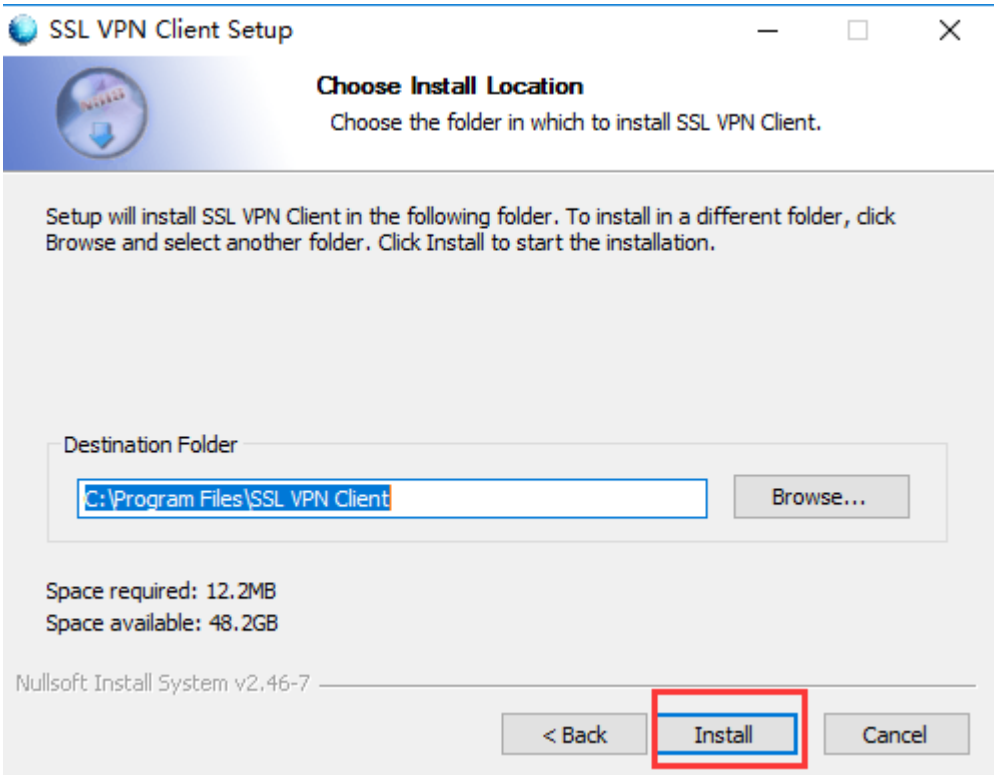
(3) 选择默认安装组件，点击“Next”进入下一步。

图1-30 选择默认安装组件



(4) 选择安装位置，点击“Install”开始安装。

图1-31 选择安装位置

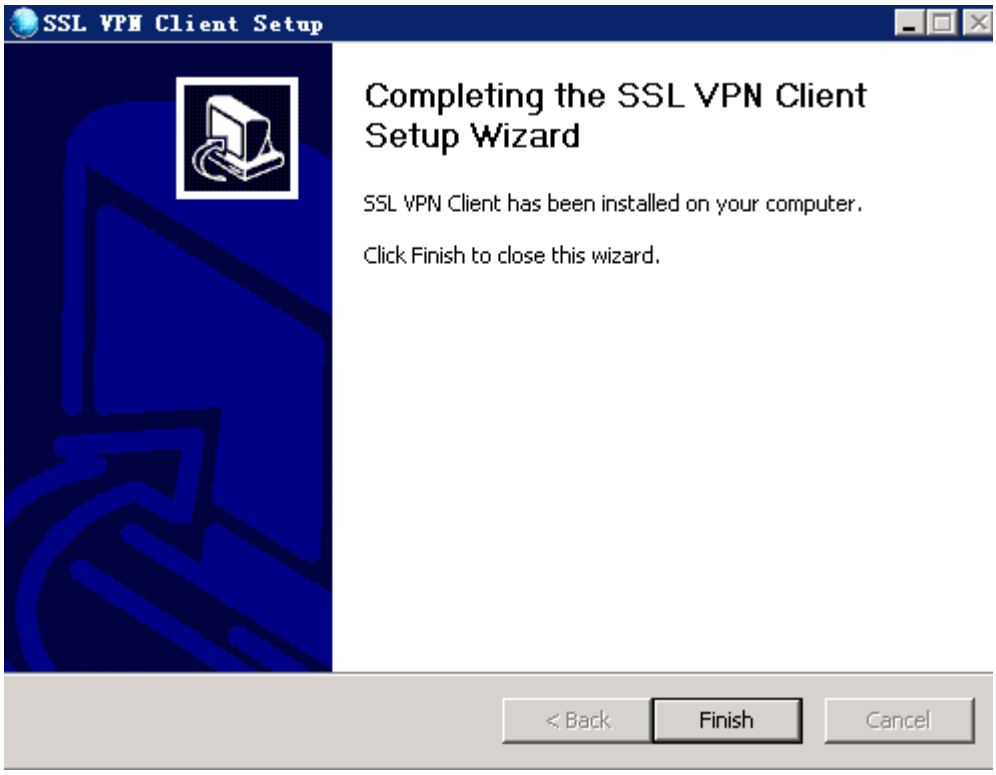


(5) 弹出安全提示页面，点击“安装”。

图1-32 安装

(6) 点击“Finish”完成安装。

图1-33 完成



2. 客户端配置

(1) 运行 SSL VPN 客户端程序

，进入添加配置文件界面，如下图所示。

图1-34 配置文件页面

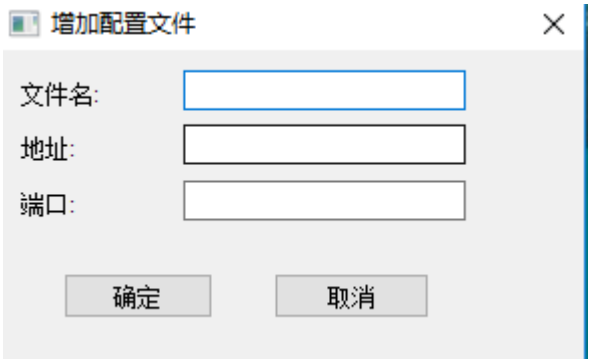


表1-9 配置文件界面详细描述

标题项	说明
文件名	添加配置文件名称，任意
地址	SSL VPN设备IP
端口	SSL VPN端口

(2) 添加完配置文件后，选择任务栏中的 图标点击右键，进行客户端连接，如下图所示。

图1-35 右键列表

表1-10 客户端设置界面详细描述

标题项	说明
连接	进行SSL VPN连接
断线	SSL VPN连接成功后断开
重新连接	SSL VPN连接成功后重连
修改密码	SSL VPN连接成功后修改登录密码
显示状态	SSLPVN连接成功后点击显示状态，弹出状态框
显示记录	点击显示记录，弹出SSL VPN连接的LOG记录
编辑配置文件	进行配置文件的修改
清除保存的密码	清除保存的SSL VPN用户密码
导入配置文件	进行配置文件的导入
新增配置文件	新建配置文件
选项	进行客户端的设置，包括：语言设置、开启是否自动启动、代理设置、配置文件以及log日志的目录、客户端版本信息
退出	关闭客户端

(3) 点击<连接>按钮，进行 SSL VPN 连接。弹出认证界面，如下图所示。

图1-36 认证界面

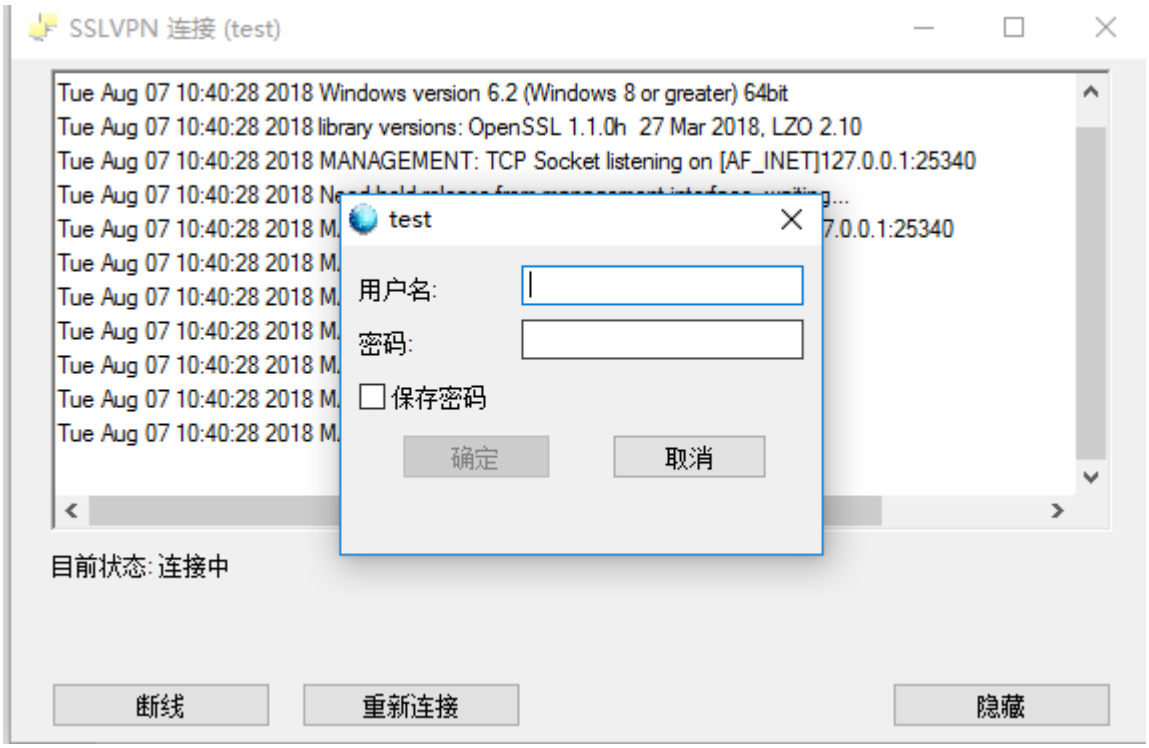


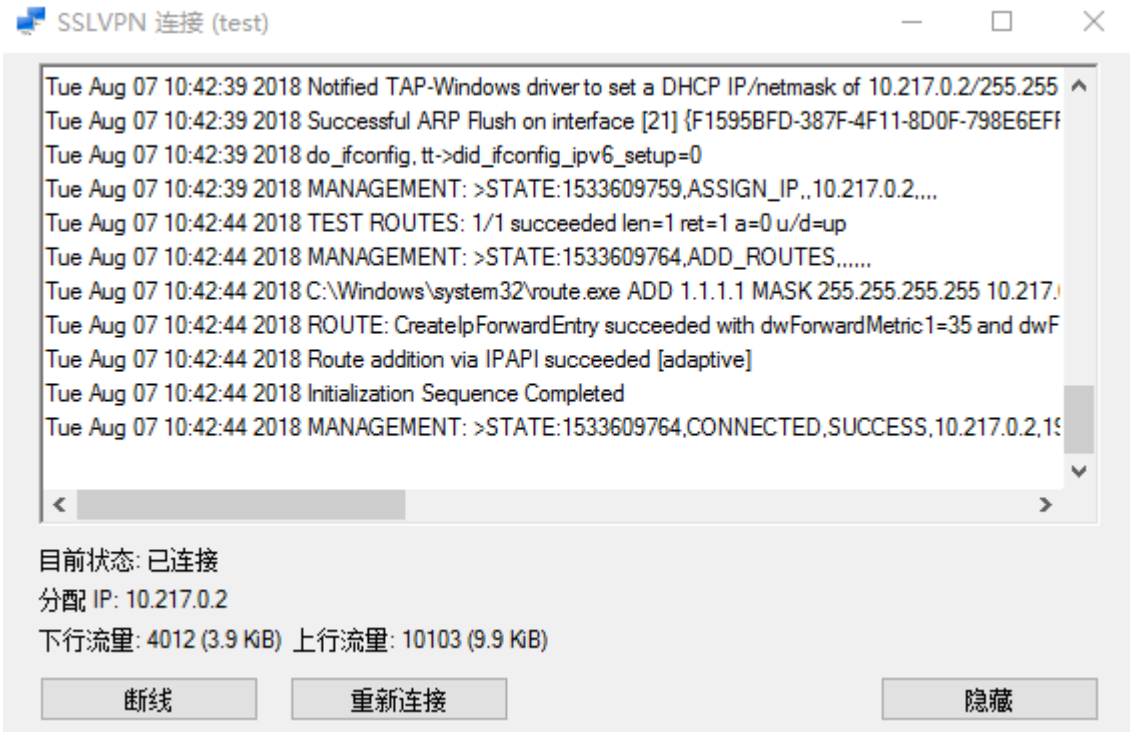
表1-11 认证界面详细描述

标题项	说明
用户名	SSL VPN登录用户名
密码	SSL VPN登录密码
保存密码	是否保存密码

(4) 输入正确的用户名密码后，SSL VPN 连接成功。SSL VPN 连接状态如图 1-37 所示，连接日志如图 1-38 所示。

图1-37 任务栏状态图

图1-38 连接日志



1.6.3 Android 系统 SSL VPN 客户端安装及配置

1. 客户端安装

(1) 将 Android 系统的 SSL VPN 客户端软件发送到手机上，点击运行安装程序。

图1-39 安装客户端

(2) 选择“继续安装”。

图1-40 继续安装

(3)　安装成功。

图1-41 安装成功

2. 客户端配置

(1)　运行 SSL VPN 客户端程序

，进入配置界面。

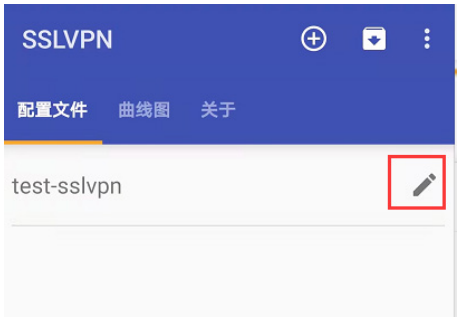
图1-42 配置客户端

(2)　点击添加图标，添加新的 VPN 配置，输入配件文件的名字。

图1-43 输入配件文件的名字

(3) 命名完成之后，点击编辑。

图1-44 编辑



(4) 编辑基础配置，输入用户名和密码。

图1-45 输入用户名和密码

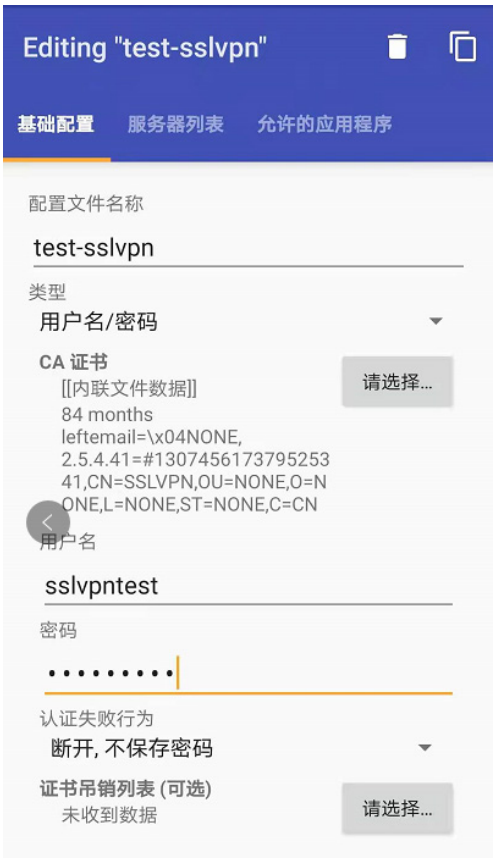


表1-12 基础配置界面详细描述

标题项	说明
用户名	SSL VPN登录用户名
密码	SSL VPN登录密码
认证失败行为	断开是否保存密码

(5) 编辑服务器列表，输入服务器地址和服务器端口：

图1-46 输入服务器地址和服务器端口

表1-13 服务器列表界面详细描述

标题项	说明
服务器地址	SSL VPN设备IP
服务器端口	SSL VPN端口

(6) 编辑允许的应用程序，默认为“VPN 用于所有的应用程序，但排除选定”。

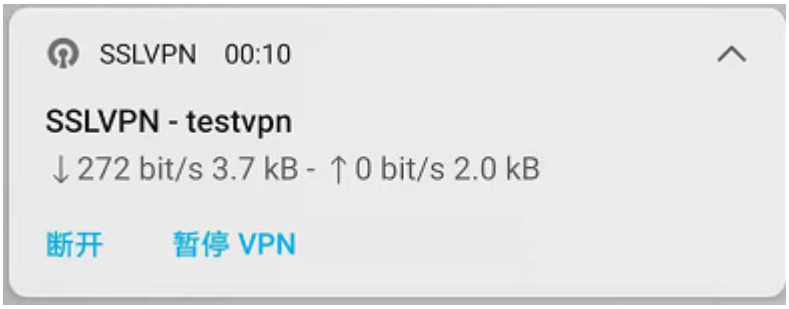
图1-47 编辑允许的应用程序

(7) 编辑完返回上级目录，点击配置文件名称“test-sslvpn”进行连接，连接成功日志如下。

图1-48 连接成功的日志

(8) 连接成功的状态，如下图所示。

图1-49 连接成功的状态



目 录

1 DHCP……1-1
1.1 DHCP 简介……1-1
1.1.1 DHCP Server……1-1
1.1.2 DHCP 中继代理(Relay)……1-2
1.2 DHCP 服务……1-2
1.3 DHCP 服务器……1-3
1.3.2 配置 DHCP IPv4 服务器……1-4
1.3.3 配置 DHCP IPv6 服务器……1-5
1.4 排除范围……1-7
1.4.2 配置 IPv4 排除范围……1-7
1.4.3 配置 IPv6 排除范围……1-8
1.5 静态地址分配……1-9
1.6 监视器……1-11
1.7 DHCP 典型配置举例……1-11
1.7.1 DHCP Server 典型配置举例……1-11
1.7.2 DHCP RELAY 典型配置举例……1-13

1 DHCP

1.1 DHCP简介

随着网络规模的扩大和网络复杂度的提高，网络配置越来越复杂，经常出现计算机位置变化（如便携机或无线网络）和计算机数量超过可分配的 IP 地址的情况。DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）就是为满足这些需求而发展起来的。

与 BOOTP 相比，DHCP 也采用客户/服务器通信模式，由客户端向服务器提出配置申请（包括分配的 IP 地址、子网掩码、缺省网关等参数），服务器根据策略返回相应配置信息，两种协议的报文都采用 UDP 进行封装，并使用基本相同的报文结构。BOOTP 运行在相对静态（每台主机都有固定的网络连接）的环境中，管理员为每台主机配置专门的 BOOTP 参数文件，该文件会在相当长的时间内保持不变。

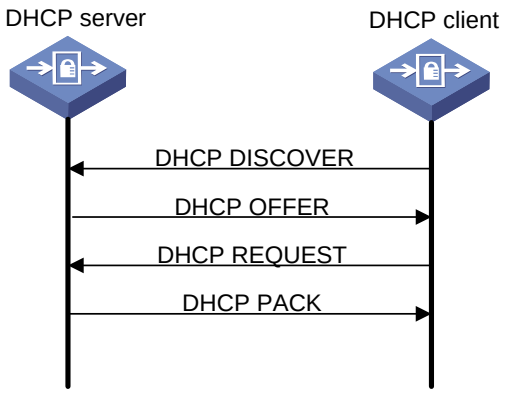
DHCP 从两方面对 BOOTP 进行了扩展：DHCP 可使计算机仅用一个消息就获取它所需要的所有配置信息；DHCP 允许计算机快速、动态地获取 IP 地址，而不是静态为每台主机指定地址。

1.1.1 DHCP Server

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）。

如图 1-1 反映了 DHCP 客户端从 DHCP Server 申请 IP 地址的过程。

图1-1 DHCP 服务器原理图



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路，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 Server，凡是具有有效 IP 地址信息的 DHCP Server 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。

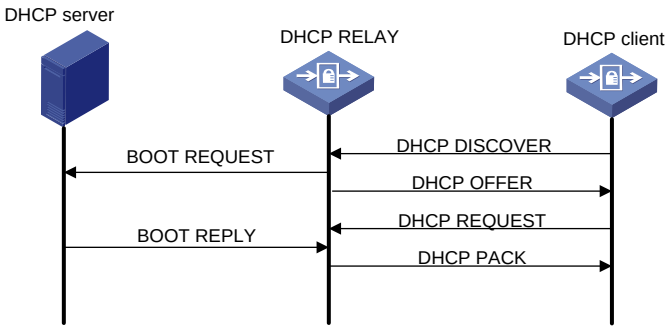
客户端从接收到的第一个提议中选定 IP 地址信息，并广播一条租用地址的消息请求。由发出该提议的 DHCP Server 响应该消息，确认已接受请求并开始租用。

客户端收到确认后开始使用此地址。

1.1.2 DHCP 中继代理(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 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。DHCP 中继代理的工作原理如图 1-2 所示。

图1-2 DHCP 代理原理图



1.2 DHCP服务

通过菜单“网络配置 > 基础网络 > DHCP 服务”，进入如图 1-3 所示页面。在该页面上，可以设置各个接口下的 DHCP 服务类型。

图1-3 DHCP 服务页面

DHCP服务 | 服务器 | 排除范围 | 静态地址分配 | 监视器

	接口	服务	中继服务器地址	操作
1	ge0	无		
2	ge1	无		
3	ge3	无		
4	ge4	无		
5	ge5	无		
6	ge6	无		
7	ge7	无		
8	ge8	无		

点击<编辑>按钮，进入如图 1-4 所示的页面，进行接口下 DHCP 服务类型的配置。各个配置项的含义如表 1-1 所示。

图1-4 接口 DHCP 服务类型配置页面

表1-1 DHCP 服务配置项含义描述表

标题项	说明
接口名称	配置DHCP服务的接口名称。
空	接口不启用任何DHCP服务。
DHCP中继代理	接口启用DHCP中继代理服务。
DHCP服务器	接口启用DHCP服务器服务。
IPv4 服务器IP	接口启用IPv4 DHCP RELAY服务后，DHCP服务器的IP地址。
DHCPv6中继代理	接口启用DHCPv6中继代理服务。
DHCPv6服务器	接口启用DHCPv6服务器服务。
IPv6路由通告	点击此链接后直接前往IPv6路由通告页面。
IPv6 服务器IP	接口启用DHCPv6中继代理服务后，DHCP服务器的IP地址。

1.3 DHCP服务器

通过菜单“网络配置 > 基础网络 > DHCP 服务 > 服务器”，进入如图 1-5 所示页面。在该页面上可以新建、编辑、删除、浏览 DHCP 服务器的配置。

图1-5 DHCP 服务器页面

1.3.2 配置 DHCP IPv4 服务器

在页面上点击“新建 > IPv4 服务器”，可以新建 DHCPv4 服务器。新建页面如图 1-6 所示。各个配置项的含义如表 1-2 所示。

图1-6 DHCPv4 服务器配置

表1-2 DHCPv4 服务器配置项含义描述表

标题项	说明
名称	DHCP服务器配置名称。
子网/掩码	DHCP服务器的子网和掩码。
网关	DHCP服务器的网关。
IP地址开始	DHCP服务器地址池的开始地址。
IP地址结束	DHCP服务器地址池的结束地址。
租约	DHCP服务器分配的地址的租约时间： • 无限：DHCP 服务器分配的 IP 地址永久有效。 • 有限期：配置有效时间，该时间内 DHCP 服务器分配的 IP 地址有效。
DNS1	DHCP服务器的主DNS。
DNS2	DHCP服务器的备DNS。
Wins1	DHCP服务器的主Wins。
Wins2	DHCP服务器的备Wins。
域	DHCP服务器的域名
AC1	DHCP服务器中option43字段AC1的IP地址。
AC2	DHCP服务器中option43字段AC2的IP地址。

点击<提交>按钮，提交配置。提交配置后可在如图 1-7 所示的页面上查看配置的 DHCPv4 服务器信息。

图1-7 DHCPv4 服务器概览

点击<编辑>按钮，可对选中条目进行编辑。

点击<删除>按钮，可对选中条目进行删除。

1.3.3 配置 DHCP IPv6 服务器

在页面上点击“新建 > IPv6 服务器”，可以新建 DHCPv6 服务器。新建页面如图 1-8 所示。各个配置项的含义如表 1-3 所示。

图1-8 DHCPv6 服务器配置

表1-3 DHCPv6 服务器配置项含义描述表

标题项	说明
名称	DHCP服务器配置名称。
子网/前缀长度	DHCP服务器的子网和前缀长度。
地址范围	DHCP服务器分配给请求IP地址的客户端的地址范围。
前缀代理	DHCP服务器分配给请求前缀的客户端的前缀范围。
可分配前缀长度	DHCP服务器分配给客户端的前缀总长度。
租约	DHCP服务器分配的地址的租约时间： • 无限：DHCP 服务器分配的 IP 地址永久有效。 • 有限期：配置有效时间，该时间内 DHCP 服务器分配的 IP 地址有效。
首选DNS服务器	DHCP服务器的主DNS。

标题项	说明
备用 DNS 服务器	DHCP 服务器的备 DNS。
Wins1	DHCP 服务器的主 Wins。
Wins2	DHCP 服务器的备 Wins。
域	DHCP 服务器的域名
SNTP 服务器	SNTP 服务器的 IP 地址。
SIP 服务器	SIP 服务器的 IP 地址。
AC1	DHCP 服务器中 option52 字段 AC1 的 IPv6 地址。
AC2	DHCP 服务器中 option52 字段 AC2 的 IPv6 地址。

点击<提交>按钮，提交配置。提交配置后可在如图 1-7 所示的页面上查看配置的 DHCPv6 服务器信息。

图1-9 DHCPv6 服务器概览

点击<编辑>按钮，可对选中条目进行编辑。

点击<删除>按钮，可对选中条目进行删除。

1.4 排除范围

通过菜单“网络配置 > 基础网络 > DHCP 服务 > 排除范围”，进入如图 1-10 所示页面。在该页面上可以新建、编辑、删除、浏览排除范围的配置。

图1-10 排除范围页面

1.4.2 配置 IPv4 排除范围

在页面上点击“新建>IPv4 排除范围”，可以新建 IPv4 排除范围。新建页面如图 1-11 所示。各个配置项的含义如表 1-4 所示。

图1-11 新建 IPv4 排除范围页面

表1-4 IPv4 排除范围各个配置项的含义描述表

标题项	说明
起始IP	排除范围的起始IPv4地址。
结束IP	排除范围的结束IPv4地址。

点击<提交>，提交配置。提交配置后可在如图 1-12 所示的页面上查看配置的 IPv4 排除范围信息。

图1-12 IPv4 排除范围页面概览

点击<编辑>按钮，可对选中条目进行编辑。

点击<删除>按钮，可对选中条目进行删除。

1.4.3 配置 IPv6 排除范围

在页面上点击“新建>IPv6 排除范围”，可以新建 IPv6 排除范围。新建页面如图 1-13 所示。各个配置项的含义如表 1-5 所示。

图1-13 新建 IPv6 排除范围页面

表1-5 IPv6 排除范围各个配置项的含义描述表

标题项	说明
起始IP	排除范围的起始IPv6地址。
结束IP	排除范围的结束IPv6地址。

点击<提交>，提交配置。提交配置后可在如图 1-12 所示的页面上查看配置的 IPv6 排除范围信息。

图1-14 IPv6 排除范围页面概览

点击<编辑>按钮，可对选中条目进行编辑。

点击<删除>按钮，可对选中条目进行删除。

1.5 静态地址分配

通过菜单“网络配置 > 基础网络 > DHCP 服务 > 静态地址分配”，进入如图 1-15 所示页面。在该页面上可以新建、编辑、删除、浏览静态地址分配的配置。

图1-15 静态地址分配页面

点击页面上的<新建>按钮，可以新建静态地址分配。新建页面如图 1-16 所示。各个配置项的含义如表 1-6 所示。

图1-16 新建静态地址分配页面

表1-6 静态地址分配各个配置项的含义描述表

标题项	说明
名称	静态地址分配的名称，可输入1到31个字符。
IP地址	静态地址分配的IPv4地址。
MAC地址	静态地址分配的MAC地址。

点击<提交>按钮，提交配置。提交配置后可在如图 1-17 所示的页面上查看配置的静态地址信息。

图1-17 IP-MA 绑定页面概览

点击<编辑>按钮，可对选中条目进行编辑。

点击<删除>按钮，可对选中条目进行删除。

1.6 监视器

当设备作为 DHCP 服务器时，可以通过监视器来查看地址池中的 IP 地址分配情况。

通过菜单“网络配置 > 基础网络 > DHCP 服务 > 监视器”，进入如图 1-18 所示页面。在该页面上可以查看 IP 地址的分配使用情况。表中各项的含义如表 1-7 所示。

图1-18 监视器页面

表1-7 监视器各项含义描述表

标题项	说明
IP地址	已分配正在使用的IP地址。
MAC地址	已分配正在使用的IP地址对应的MAC地址。
开始时间	已分配正在使用的IP地址的开始使用时间。
结束时间	已分配正在使用的IP地址的回收时间。

点击<清除>按钮，可以清除已分配的 IP 地址。

1.7 DHCP典型配置举例

1.7.1 DHCP Server 典型配置举例

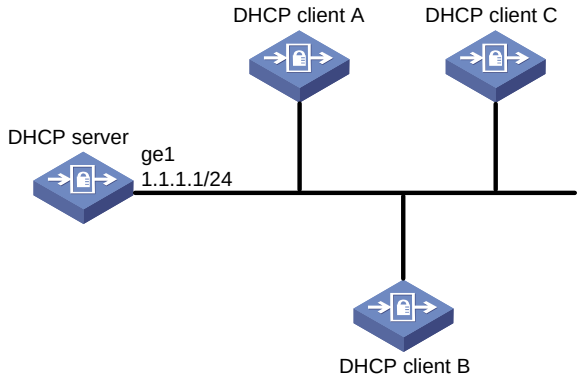
1. 组网需求

客户端通过 DHCP Server 获取动态 IP 地址。

- DHCP 客户端和设备在同一局域网内。
- DHCP 客户端启用自动获取 IP 地址。

2. 组网图

图1-19 DHCP Server 组网图



3. 配置步骤

(1) 按照组网图组网。

(2) 设备接口配置为 DHCP Server。如图 1-20 所示。

图1-20 接口 ge1 配置为 DHCP SERVER

DHCP服务 | 服务器 | 排除范围 | 静态地址分配 | 监视器

	接口	服务	中继服务器地址	操作
1	ge0	无		
2	ge1	DHCP服务器		
3	ge3	无		
4	ge4	无		
5	ge5	无		
6	ge6	无		
7	ge7	无		
8	ge8	无		
9	agg0	无		
10	ge1.1	无		
11	bvi0	无		

(3) 配置 DHCP Server。如图 1-21 所示。

图1-21 配置 DHCP 地址池

点击<提交>按钮，提交配置。

4. 验证配置

配置完成后，在 PC 上查看 IP 地址获取情况，看到 PC 获取到 IP 地址为 1.1.1.2，DNS 为 8.8.8.8 和 8.8.4.4。

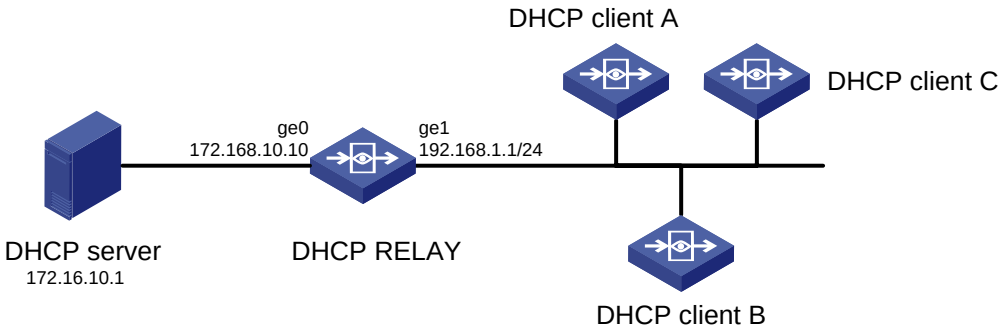
1.7.2 DHCP RELAY 典型配置举例

1. 组网需求

客户端通过 DHCP RELAY 获取动态 IP 地址。

- PC 和设备在同一局域网内。
- PC 启用自动获取 IP 地址。
- 设备所在的另一网段内存在有 DHCP Server。

图1-22 DHCP RELAY 组网图



2. 配置步骤

(1) 按照组网图组网。

(2) 设备配置为 DHCP RELAY。如图 1-23 所示。

图1-23 DHCP RELAY 配置页面

点击<提交>，提交配置。

3. 验证配置

配置完成后，在 PC 上查看 IP 地址获取情况，看到 PC 获取到由 DHCP Server 分配的 IP 地址，及 DNS。

目 录

1 DNS ····· 1-1
1.1 DNS 简介 ····· 1-1
1.2 DNS 域名管理 ····· 1-1
1.3 动态缓存配置 ····· 1-2
1.4 特定域名解析配置 ····· 1-3
1.5 DNS 透明代理配置 ····· 1-4
1.5.2 DNS 服务器配置 ····· 1-5
1.6 DNS 典型配置举例 ····· 1-6
1.6.1 DNS 典型配置举例 ····· 1-6

1 DNS

1.1 DNS简介

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）。DNS 协议运行在 UDP 协议之上，使用端口号 53。

本功能具有如下功能点：

- 能够根据用户的 DNS 请求，从本地查找 DNS 缓存，然后对用户的请求做出应答。
- 能够向配置的远端 DNS server 请求，然后对用户的请求做出应答。
- 能够手动配置 DNS 域名，方便对一些 IP 地址的访问。
- 能够对设备本身的 DNS 请求，做出 DNS 域名解析。

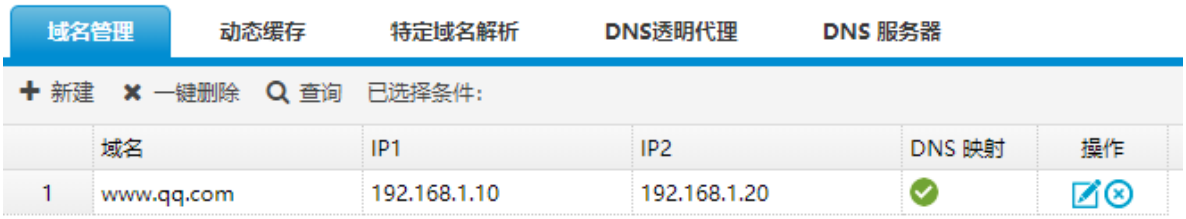
说明

DNS 模块缓存数量并非无限，可缓存最多条目数根据设备自身的规格而定，并且规格中总存储条目数中，有 256 条，用于保存静态域名配置。

1.2 DNS域名管理

通过菜单“网络配置 > 基础网络 > DNS 服务 > 域名管理”，进入如图 1-1 所示的页面。在该页面上，可以新建、编辑、删除、浏览静态域名配置项。

图1-1 域名管理展示页面



单击“新建按钮”，进入如图 1-2 所示的静态域名配置页面。各个配置项的含义如表 1-1 所示。

图1-2 域名管理配置页面

表1-1 域名管理配置说明

参数	说明
域名	静态域名信息，可以输入4到253个字符，可填入英文大小写字符、“-”、“.”，每级域名不超过63个字符。
IP1	静态域名对应的第一个IP地址，支持IPv4和IPv6地址。
IP2	静态域名对应的第二个IP地址，支持IPv4和IPv6地址。
DNS映射	DNS Mapping功能，私网用户希望通过域名访问位于同一私网的内部服务器，启用后设备会直接回复静态域名配置的IP地址，无需开启DNS透明代理或DNS全局代理。
目标位置	静态域名对应的目标位置，1-128的整数。可通过选择数字大小来调整静态域名位置。

1.3 动态缓存配置

通过菜单“网络配置 > 基础网络 > DNS 服务 > 动态缓存”，进入如图 1-3 所示的页面。在该页面上，可以开启关闭 DNS 动态缓存。该页面各展示项介绍见表 1-2。

图1-3 动态缓存配置页面

表1-2 动态缓存页面介绍

参数	说明
域名	设备解析成功的域名显示。
命中次数	DNS记录在本生存时间内被匹配的次数。
TTL	一条DNS记录的生存时间。
IP	解析成功的域名对应的IP，页面支持显示4个具体ip地址，后面（）显示总的ip地址个数。

1.4 特定域名解析配置

通过菜单“网络配置 > 基础网络 > DNS 服务 > 特定域名解析”，进入如图 1-4 所示的页面。在该页面上，可以新建、编辑、删除、浏览特定域名配置项。

图1-4 特定域名解析展示页面

单击“新建按钮”，进入如图 1-5 所示的特定域名配置页面。各个配置项的含义如表 1-3 所示。

图1-5 特定域名解析配置页面

表1-3 特定域名解析配置说明

参数	说明
域名	特定域名信息，可以输入4到253个字符，可填入英文大小写字符、“-”、“.”，每级域名不超过63个字符。
主DNS	特定域名对应的第一个DNS服务器地址。
备DNS	特定域名对应的第二个DNS服务器地址。
目标位置	特定域名对应的目标位置，1-128的整数。可通过选择数字大小来调整静态域名位置。

1.5 DNS透明代理配置

通过菜单“网络配置 > 基础网络 > DNS 服务 > DNS 透明代理”，进入如图 1-6 所示的页面。在该页面上，可以新建、编辑、删除、启用、设置均衡值标准、浏览 DNS 透明代理配置项。

图1-6 DNS 透明代理展示页面

单击“新建按钮”，进入如图 1-7 所示的 DNS 透明代理配置页面。各个配置项的含义如表 1-4 所示。

图1-7 DNS 透明代理配置页面

表1-4 DNS 透明代理配置说明

参数	说明
DNS链路	DNS出接口名称例如：GE0。
DNS链路均衡值	权重、优先级和流量的数值，取值范围为：1-100。
DNS模式选择	透明代理的规则分为2种类型：手工配置和自动链路继承。手工配置是指对于配置有IP地址的三层网络接口，需要人为的配置正确的DNS服务器地址才能正常域名解析的类型。自动链路继承是指对于配置为DHCP或PPPOE类型的网络接口，既可以人为配置DNS服务器地址也可以从地址服务器端获取DNS服务器地址的类型。
主DNS	第一个DNS服务器IP。
备DNS	第二个DNS服务器IP。

1.5.2 DNS 服务器配置

- 操作步骤

通过菜单“网络配置 > 基础网络 > DNS 服务 > DNS 服务器”，进入如图 1-8 所示的页面。在该页面上，可以启用禁用 DNS 代理、编辑 DNS 服务器配置项。无论启用或禁用，各个 DNS 服务器是设备本身请求域名解析的服务器地址。各个配置项的含义如表 1-5 所示。

图1-8 DNS 服务器配置页面

表1-5 DNS 服务器配置说明

标题项	说明
启用DNS代理	启用或关闭DNS服务，当PC的DNS指向设备时充当DNS服务器代理功能
DNS服务器1	远端DNS服务器1，设备第一次解析DNS请求时，将向该DNS服务器请求

标题项	说明
DNS服务器2	远端DNS服务器2，DNS服务器1解析失败时，将向该DNS服务器请求
DNS服务器3	远端DNS服务器3，DNS服务器1和2解析失败时，将向该DNS服务器请求
DNS服务器4	远端DNS服务器4，DNS服务器1、2、3解析失败时，将向该DNS服务器请求

1.6 DNS典型配置举例

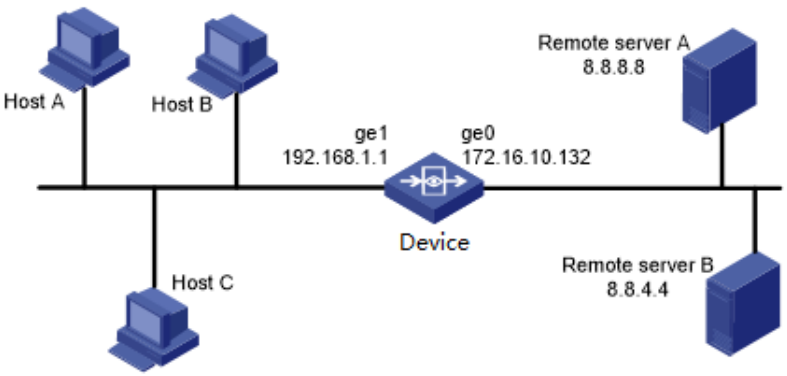
1.6.1 DNS 典型配置举例

1. 组网需求

- 内网主机将自身 DNS 服务器指向设备，设备向配置的远端 DNS 服务器进行 DNS 请求，最终设备将远端 DNS 服务器响应的域名对应的 IP 返回给内网主机。
- 设备与 Remote server 网络可达。

2. 组网图

图1-9 局域网用户组网图



3. 配置步骤

(1) 按照组网图组网。

(2) 设备配置，如图 1-10 所示。

图1-10 DNS 服务器配置

点击<提交>按钮，提交配置。

(3) 主机配置 DNS 为 192.168.1.1。

4. 验证配置

配置完成后，从主机打开浏览器，访问 www.baidu.com，设备响应主机的 DNS 请求，最终可正常打开百度的主页。

说明

设备自身有 DNS 请求时，配置类似，但只需要配置 Remote server 地址即可，不需要启用 DNS。

目 录

1 DDNS……1-1
1.1 DDNS 简介……1-1
1.2 DDNS 配置……1-1
1.3 DDNS 典型配置举例……1-2
1.3.1 DDNS 典型配置举例……1-2

1 DDNS

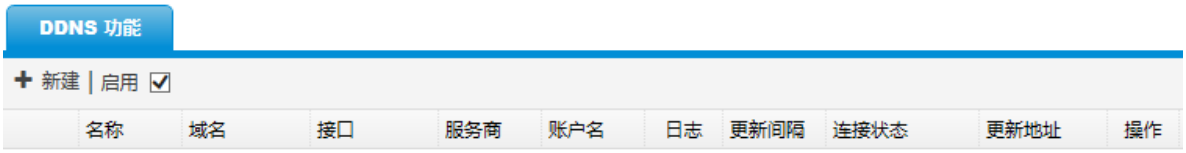
1.1 DDNS简介

DDNS 是对域名绑定的 IP 地址进行动态更新，解决网络中已注册域名的服务器的 IP 地址是动态变化的，服务器公网 IP 变更时，导致 DNS 域名服务器所绑定的该服务器的 IP 地址已经过时，用户通过域名方式无法正常访问该服务器的相关服务。设备开启 DDNS 功能后，通过更新报文把动态 IP 地址信息发送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析；保证网络可以通过此域名正常访问到服务器。

1.2 DDNS配置

通过菜单“网络配置 > 基础网络 > DDNS 服务”，进入如图 1-1 所示的页面。在该页面上，可以启用、关闭 DDNS 功能。

图1-1 DDNS 功能配置页面



点击<新建>按钮，进入如图 1-2 所示的 DDNS 条目配置页面。各个配置项的含义如表 1-1 所示。

图1-2 DDNS 条目配置页面

表1-1 DDNS 条目配置项含义

标题项	说明
名称	DDNS条目名称。
域名	所要更新此账户下的域名，若不配置则默认更新此账户下所有的域名。服务商选择阿里云时，域名必须填写，且只支持三级域名。
接口	连接外网的接口。
服务商	DDNS服务商，目前支持花生壳和阿里云。
账户名	在DDNS服务商注册的账户名。服务商为阿里云时，账户名需填写AccessKeyID。
账户密码	在DDNS服务商注册的账户所使用的密码。服务商为阿里云时，账户名需填写AccessKeySecret。
日志	开启后发送系统日志。
更新间隔	更新报文发送的时间间隔。

配置完成后，如图 1-3 所示。

图1-3 DDNS 配置完成效果

1.3 DDNS典型配置举例

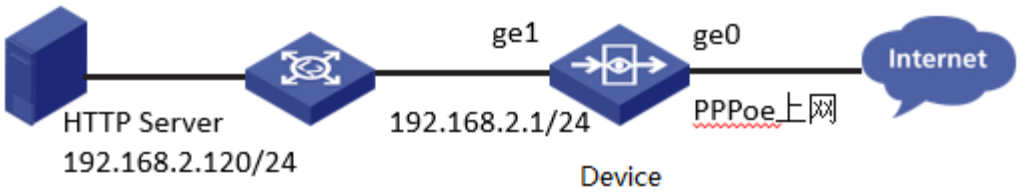
1.3.1 DDNS 典型配置举例

1. 组网需求

如下图所示，有一条公网 PPPOE 线路 WLAN 接口，内网服务器提供 HTTP 服务；具体应用需求如下：

- DDNS 实现域名 IP 动态绑定。
- 目的 NAT 实现对内网服务器进行地址映射。
- 在 WLAN 接口公网 IP 变化的情况下，仍可通过域名方式正常访问内网 HTTP 服务。

图1-4 组网图



2. 配置思路

(1) 配置 DNS 服务器。

(2) 启用 DDNS 功能，配置动态域名服务 DDNS。

(3) 配置目的 NAT，将动态域名映射到内网服务器。

3. 配置步骤

(1) 配置 DNS 服务器，保证设备能够正常进行域名解析。

如下图所示，在导航栏选择“网络配置 > 基础网络 > DNS 服务 > DNS 服务器”，配置 DNS 服务器为 114.114.114.114，点击<提交>。

图1-5 配置 dns 服务器

(2) 配置 DDNS 功能

如下图所示，在导航栏选择“网络配置 > 基础网络 >DDNS 服务”。勾选启用选项，点击确定。

图1-6 启用 DDNS 功能

如下图所示，在导航栏选择“网络管理>DDNS 服务”。点击<新建>，配置名称为 test，域名为 ***test.iask.in，接口为 ge0，服务商为花生壳，更新间隔 30，点击<提交>。

图1-7 配置动态域名服务 DDNS

如下图所示，创建成功设备将与花生壳服务商进行连接，成功后会根据配置的更新间隔发送更新报文进行更新，并显示当前更新的公网 IP 地址。

图1-8 DDNS 功能状态显示

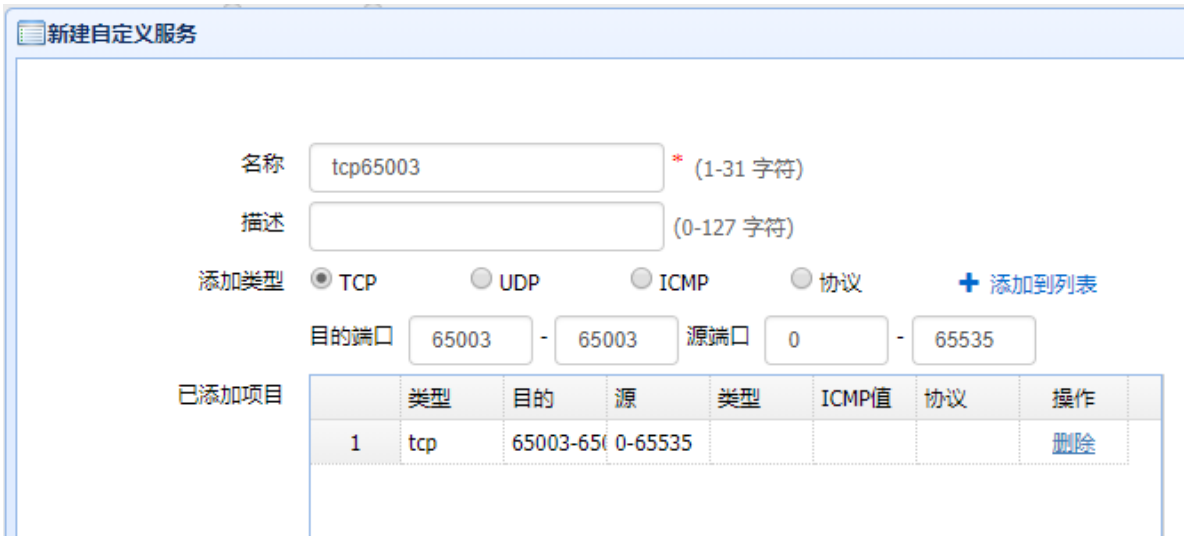
(3) 配置目的 NAT，将动态域名映射到内网服务器。

如下图所示，在导航栏选择“策略配置>对象管理>地址对象>IPv4 地址对象”。点击<新建>，配置域名为***test.iask.in，点击<提交>。

图1-9 配置地址对象

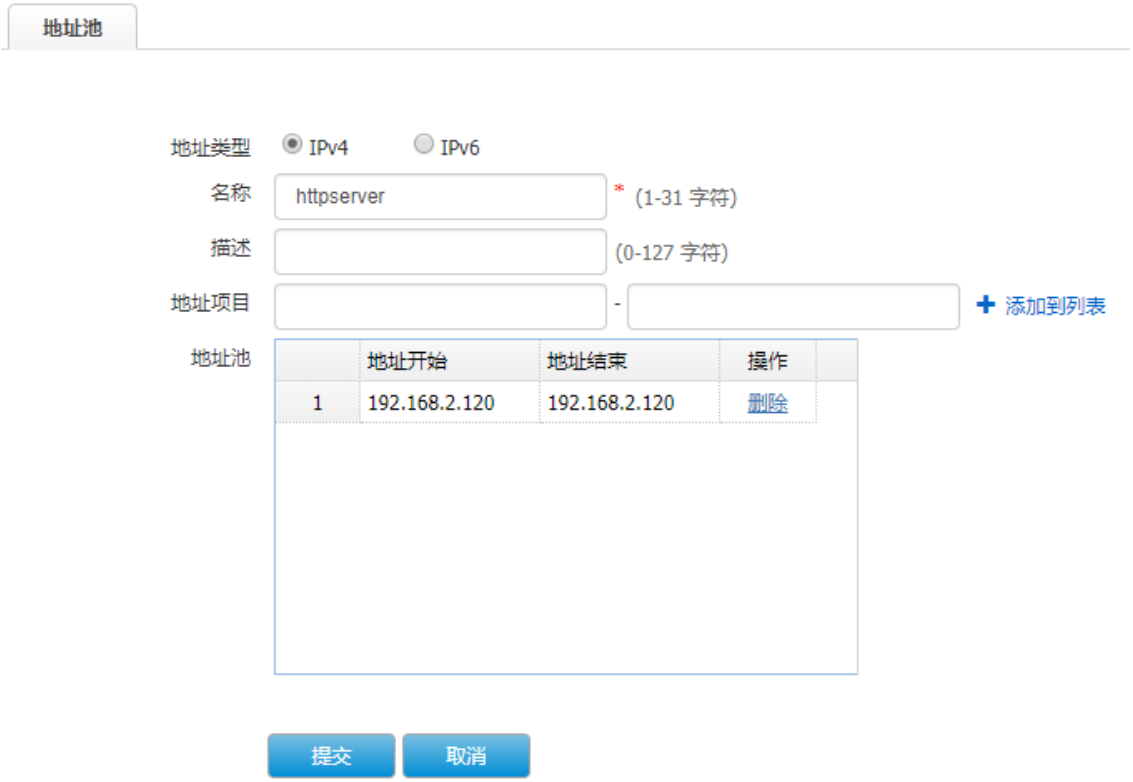
如下图所示，在导航栏选择“策略配置>对象管理>服务对象>自定义服务”。点击<新建>，配置名称为 tcp65003，目的端口 65003-65003，源端口 0-65535 的自定义服务对象，点击<提交>。

图1-10 配置自定义服务



如下图所示，在导航栏选择“策略配置 > NAT 转换策略 > 地址池”。点击<新建>，配置名称为 httpserver，地址池的地址类型为 IPv4，地址项目为 192.168.2.120，点击<提交>。

图1-11 配置地址池



如下图所示，在导航栏选择“策略配置 > NAT 转换策略 > 目的 NAT”。点击<新建>，配置源地址为 any，目的地址为地址对象***test.iask.in,服务为自定义服务 tcp65503,接口为 ge0，转换后 IP 为 httpserver，转换后端口为 80，点击<提交>。

图1-12 配置目的 NAT

目的 NAT 配置完成后显示如下图所示。

图1-13 目的 NAT

如图所示，在导航栏选择“网络配置 > 基础网络 >DNS 服务 > DNS 透明代理”，点击<新建>，配置 DNS 代理相关参数。

图1-14 DNS 透明代理

点击<提交>按钮，提交配置。

在导航栏选择“网络配置 > 基础网络 >DNS 服务 > 域名管理”，点击<新建>配置静态域名，如图1-15 所示。

图1-15 配置域名管理

在导航栏选择“网络配置 > 基础网络 > DNS 服务 > 特定域名解析”，点击<新建>，配置特定域名解析相关信息，如图 1-16 所示。

图1-16 配置特定域名

在导航栏选择“网络配置 > 基础网络 > DNS 服务 > DNS 服务器”，勾选<启用代理>，配置代理服务器地址，如图 1-17 所示。

图1-17 配置全局 DNS 服务器

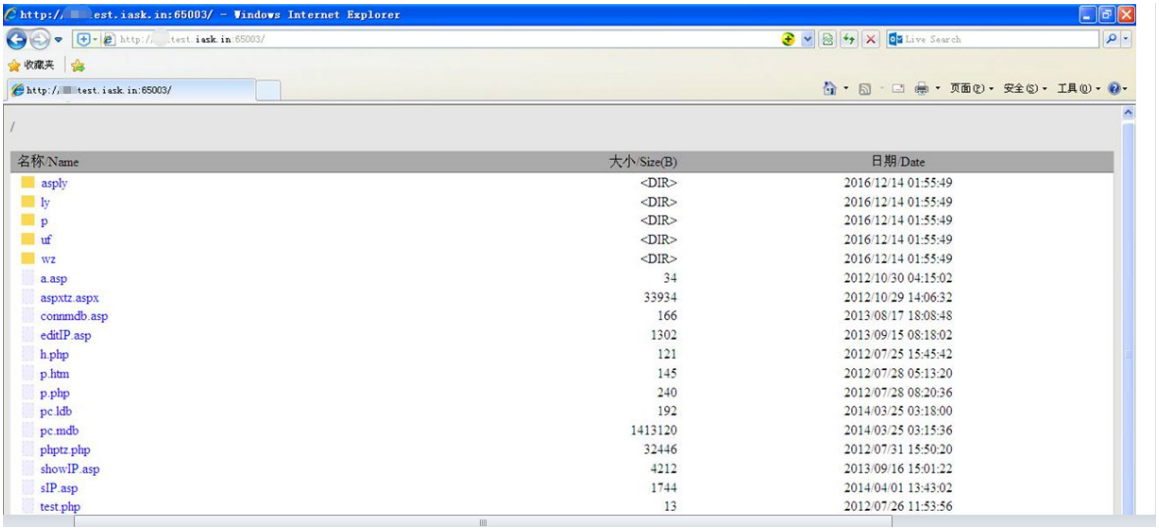
在导航栏选择“网络配置 > 基础网络 > DNS 服务”，选择动态缓存页面，勾选<启用>开启域名动态缓存功能，如图 1-18 所示。

图1-18 开启动态缓存

4. 验证配置

如下图所示，在 Internet 访问 http:// ***test.iask.in:65003，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。

图1-19 通过域名访问内网 HTTP 服务器



目 录

1 应用缓存 ····· 1-1
1.1 概述 ····· 1-1
1.2 配置 ····· 1-1
2 APP 动态缓存 ····· 2-2
2.1 概述 ····· 2-2
2.2 配置 ····· 2-2
3 配置举例 ····· 3-4
3.1 应用缓存配置举例 ····· 3-4
3.2 APP 动态缓存配置案例 ····· 3-5

1 应用缓存

1.1 概述

应用缓存功能，是以网络节点（比如网关设备）作为锚点，该功能的开启，首先将用户需求的应用软件（一般是用户高频使用的软件，例如：QQ、微信等）上传到该锚点。随后配置相应的 URL 链接并与上传的应用完成一一对应。

当用户接入网络发起对应用软件（例如：QQ）的下载时，则命中该锚点上的 URL，则用户直接从该锚点下得该应用。

对于用户来讲，通过应用缓存下载软件会比在互联网下载速度要快。

该功能有两种配置方式分别为精确匹配和模糊匹配。

1. 精确匹配

只有下载的 http 地址（URL）与配置的 URL 地址完全一致时，才会命中已经缓存在设备上的 APP 文件，实现 APP 文件加速下载的功能。

2. 模糊匹配

目前市场上发现安卓应用缓存 URL 在变化，为了应对这种场景，可以开启模糊匹配功能。

截取完整 URL 中的部分路径（比如取用 URL 的 path 部分）作为模糊匹配的 URL 条件，从而达到在精确匹配的基础上进行更为宽松匹配的一种方式。

1.2 配置

点击导航栏的“网络配置 > 基础网络 > 应用缓存”，进入应用缓存的显示页面，如图 1-1 所示。在应用缓存页面中，点击<新建>按钮，会切换到新建的页面，如图 1-2 所示。

图1-1 应用缓存显示界面

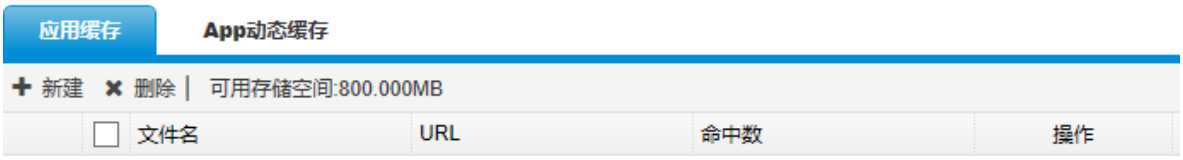


图1-2 应用缓存配置页面

表1-1 应用缓存详细信息描述表

配置项	说明
模糊匹配	勾选则开启模糊匹配，不勾选则使用精确匹配，默认为不勾选。
URL	资源对象网络地址，精确匹配的URL需要输入标准的url格式（必须包括路径或文件名），例如：http://www.qq.com/qq.exe。
上传文件名称	资源对象名称。

2 APP 动态缓存

2.1 概述

APP 动态缓存截取现网用户在应用商城内下载文件的下载 URL，自身再次请求下载此文件或其它用户若下载相同文件时，将进入设备动态缓存下载到的文件通道进行下载，不在网络当中占用带宽下载。

2.2 配置

通过界面“网络配置 > 基础网络 > 应用缓存 > APP 动态缓存”，进入如图 2-1 所示的页面。在该页面上，可以新建 app 动态缓存。

图2-1 App 动态缓存页面

注意

开启此功能前，请先配置 dns 服务器。

单击“新建”按钮，添加缓存域名，如图 2-2 所示，各个配置项的含义如表 2-1 所示。

图2-2 添加缓存域名

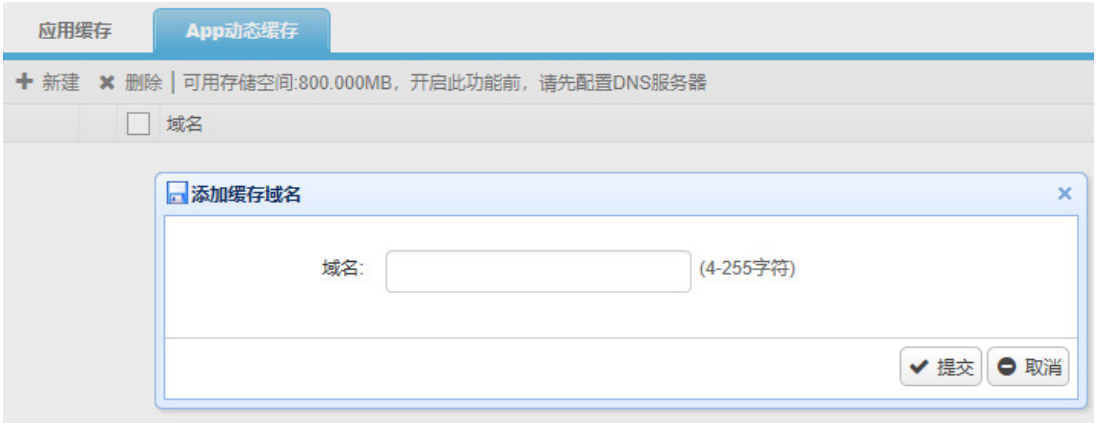
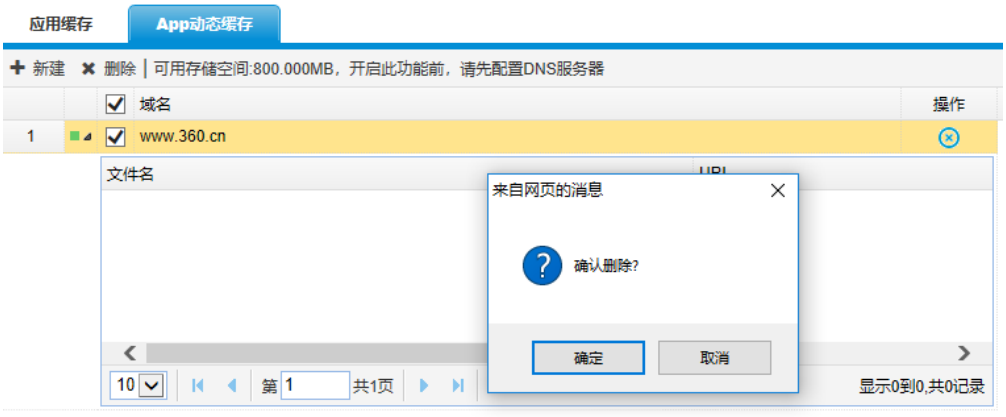


表2-1 添加缓存域名说明

参数	说明
域名	添加应用商城的下载域名，字符限制在4-255内合法字符。

选中要删除的域名，单击“删除”按钮，可以删除已添加的域名，如图 2-3 所示。

图2-3 删除已加的域名



3 配置举例

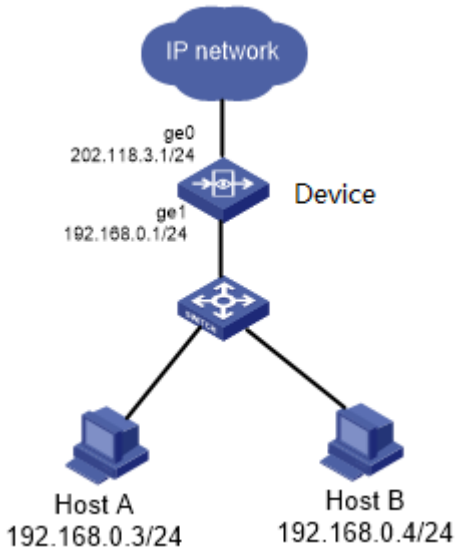
3.1 应用缓存配置举例

1. 组网需求

各设备接口及主机的 IP 地址和掩码如图 3-1 所示。测试用户 HostA，HostB 通过设备正常上网。

2. 组网图

图3-1 应用缓存-精确匹配的配置案例组网图



3. 配置步骤

(1) 按照组网图组网。

(2) 通过菜单“网络配置 > 基础网络 > 应用缓存”，点击<新建>，按照如图 3-2 所示配置精确匹配。

图3-2 精确匹配配置

点击<提交>按钮，提交配置。

4. 验证配置

查看应用缓存的命中数，验证是否生效，如图 3-3。

图3-3 验证配置

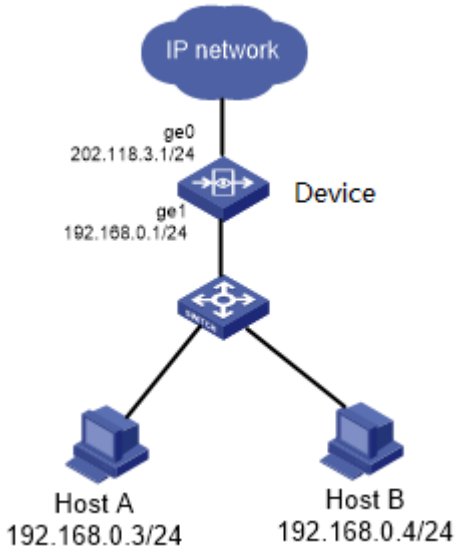
3.2 APP动态缓存配置案例

1. 组网需求

设备接口及主机的 IP 地址和掩码如图 3-4 所示，测试用户 HostA，HostB 通过设备正常上网。在设备上配置 www.icbc.com.cn 的动态缓存功能，使设备能够自动缓存对应的 APP。

2. 组网图

图3-4 APP 动态缓存配置案例组网图

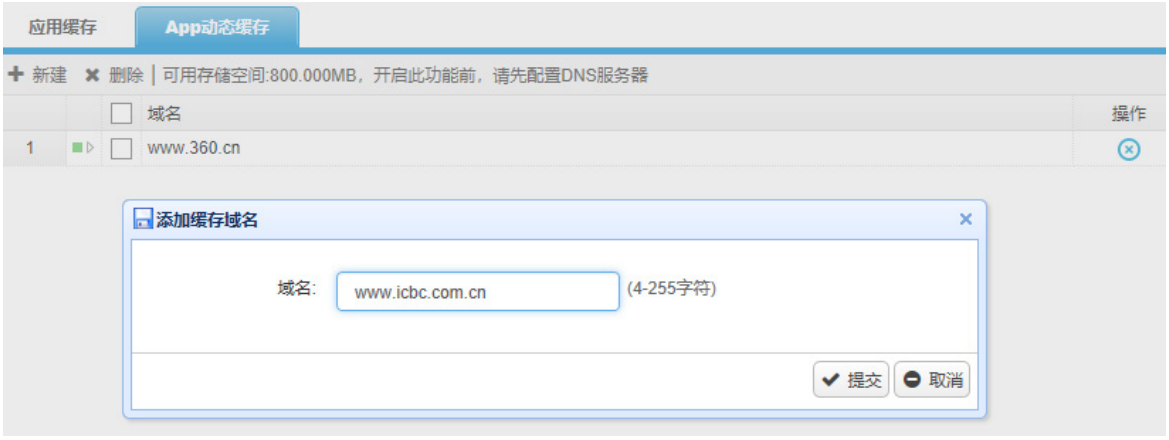


3. 配置步骤

(1) 按照组网图组网。

(2) 通过菜单“网络配置 > 基础网络 > 应用缓存 > APP 动态缓存”，点击<新建>，按照如图 3-5 所示配置 APP 动态缓存匹配。

图3-5 动态缓存配置

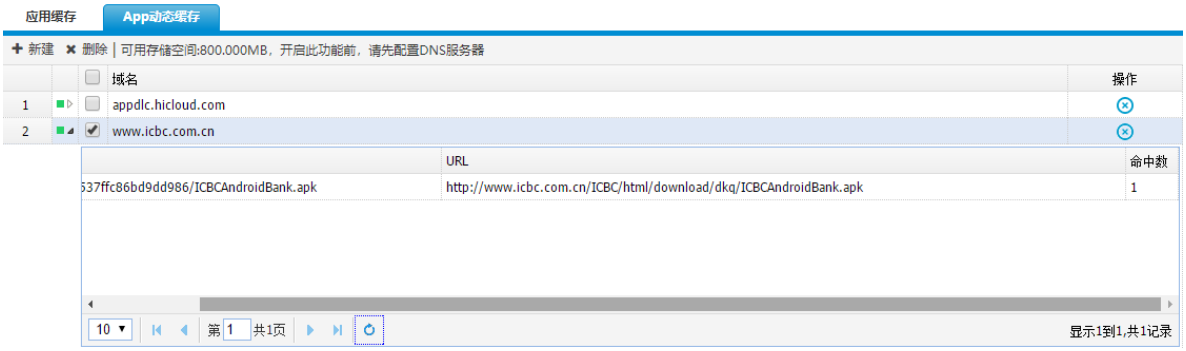


填写相应的域名后，点击<提交>按钮，提交配置。

4. 验证配置

测试用户 HOSTA 和用户 HOSTB，通过访问如下 URL 下载 app：（http://www.icbc.com.cn/ICBC/html/download/dkq/ICBCAndroidBank.apk），查看 APP 动态缓存的下载文件名，下载文件的 URL，命中数，验证是否生效，如图 3-6 所示。

图3-6 验证配置


应用缓存
App动态缓存
新建
删除 | 可用存储空间:800.000MB，开启此功能前，请先配置DNS服务器
域名
操作
1
appdlc.hicloud.com
2
www.icbc.com.cn
URL
命中数
637ffc86bd9dd986/ICBCAndroidBank.apk
http://www.icbc.com.cn/ICBC/html/download/dkq/ICBCAndroidBank.apk
1
10
第 1 共1页
显示1到1,共1记录

目 录

1 服务质量管理 ····· 1-1
1.1 概述 ····· 1-1
1.2 配置 ····· 1-1
1.3 配置案例 ····· 1-2

1 服务质量管理

1.1 概述

服务质量管理是指，通过配置接口、协议、目的地址、端口号、探测间隔等信息后，由设备定时发送对应的探测报文，并解析返回的响应报文，作为一个采样点。定时对一个时间段内的采样点进行统计分析，计算出该时间段的探测成功率，和该时间段内的平均延时。再将这些统计结果，在页面中通过曲线表现出来，方便网络管理员了解当前或者过去某一个时刻的网络状况，更加方便有效的管理维护网络。

本功能具有如下功能点：

- 可配置 PING、DNS 探测条目。
- 可配置 TCP 协议，通过配置端口号，可添加 HTTP、FTP、E-mail 的探测条目。
- 收集每个探测条目的请求总次数，成功总次数，计算成功比例。以 10 分钟为单位统计。保留一周的数据，以文件形式保存。
- 收集每个探测条目每次探测的延时，10 分钟为单位，取平均值，保留一周的数据。
- 每个条目都对应有成功率曲线、延时曲线。且每条曲线可选择一天，或一周的显示周期。

说明

探测间隔为可配置项，统计间隔为固定 10 分钟。

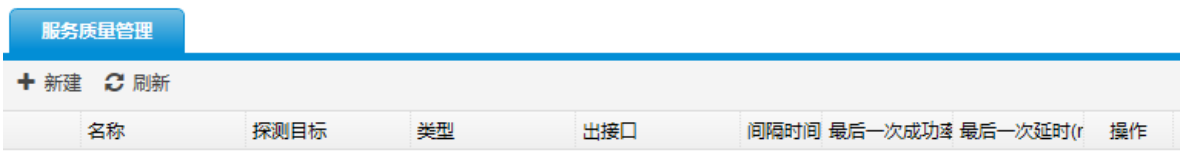
最多可配置 20 个条目。

最多保存一周的数据，达到数据上限后，新数据会覆盖旧数据。

1.2 配置

通过菜单“网络配置 > 基础网络 > 服务质量管理”，进入如图 1-1 所示的页面。在该页面上，可以新建服务质量管理。

图1-1 服务质量管理页面



点击“新建”，进入如图 1-2 所示的服务质量管理配置页面，各个配置项的含义如表 1-1 所示。

图1-2 服务质量管理配置页面

表1-1 服务质量管理配置项含义

标题项	说明
名称	服务质量管理条目名称
探测目标	服务质量管理探测地址，可以为IP地址，或域名
类型	探测条目类型，可以为PING、DNS、TCP
出接口	探测条目的发送接口 any：根据路由自动选择一个路由可达接口
间隔时间	探测条目的发送间隔时间，秒为单位

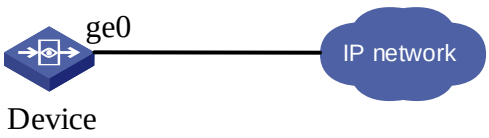
1.3 配置案例

1. 组网需求

网络连通。

2. 组网图

图1-3 服务质量管理组网图



3. 配置步骤

(1) 按照组网图组网。

点击服务质量管理配置页面的“新建”，如图 1-4 所示。

图1-4 服务质量管理配置

点击<提交>按钮，完成添加服务质量管理配置。

4. 验证配置

随着时间的推移，网络质量采样点会逐渐增加。点击服务质量管理页面中“最后一次成功率”及“最后一次延时”对应的数据，即可得到成功率曲线图，和延时曲线图。

说明

成功率曲线图，延时曲线图均可选择按天显示，或按周显示。

目 录

1 端口镜像 ····· 1-1
1.1 概述 ····· 1-1
1.2 配置端口镜像 ····· 1-1
1.2.1 新建端口进行规则 ····· 1-1
1.2.2 修改端口镜像规则 ····· 1-2
1.2.3 删除端口镜像规则 ····· 1-3
1.3 端口镜像典型配置举例 ····· 1-4
1.3.1 组网需求 ····· 1-4
1.3.2 配置步骤 ····· 1-4
1.3.3 验证配置 ····· 1-5

1 端口镜像

1.1 概述

端口镜像（port Mirroring）功能是网络设备上常用的功能，将一个或多个端口的数据流量复制到某一个指定端口来实现对网络的监控。在不影响源端口正常吞吐流量的情况下，可以通过镜像端口对网络的流量进行监控分析。

端口镜像功能是对网络流量监控的一个有效的安全手段，对监控流量进行分析和安全性的检查，同时也能及时的在网络发生故障时进行准确的定位。端口镜像功能简单地说就是将被监控流量镜像到监控端口，以便对被监控流量进行故障定位、流量分析、流量备份等，监控端口一般直接与监控主机等相连。端口镜像功能能够将进出网络的所有数据包，供安装了监控软件的管理服务器抓取数据。而企业出于信息安全、保护公司机密的需要，也迫切需要网络中有一个端口能提供这种实时监控功能。在企业中用端口镜像功能，可以很好的对企业内部的网络数据进行监控管理，在网络出现故障的时候，可以做到很好地故障定位。

1.2 配置端口镜像

1.2.1 新建端口进行规则

通过菜单“网络配置>基础网络>端口镜像”，单击“新建”按钮，进入如图 1-1 所示界面，在该界面，可以新建端口镜像规则，各个配置项的含义如表 1-1 所示。

图1-1 新建端口镜像规则配置界面

表1-1 端口镜像规则配置项含义

参数	说明
名称	端口镜像规则的名称，1-31字符。
源接口	允许把此接口的流量镜像到监控接口。
监控接口	即目的接口，允许把源接口的流量镜像到的接口，不允许配置为管理口。
规则类型	根据端口镜像作用的接口模式来划分，分为以下三种类型： 入流量，只对从源接口接收的流量进行镜像。 出流量，只对从源接口发出的流量进行镜像。 双向流量，对源接口接受和发出的双向流量进行镜像。

1.2.2 修改端口镜像规则

通过菜单“网络配置>基础网络>端口镜像”，单击所要修改的规则操作中的“编辑”按钮，进入如图 1-2 所示的界面，在该界面上，可以修改端口镜像规则，各个配置项的含义如表 1-2 所示。

图1-2 修改端口镜像规则配置界面

表1-2 端口进项规则配置含义

参数	说明
名称	端口镜像规则的名称，不允许进行修改，显示为灰色。
源接口	允许把此接口的流量镜像到监控接口。
监控接口	即目的接口，允许把源接口的流量镜像到目的接口，不允许配置为管理口。

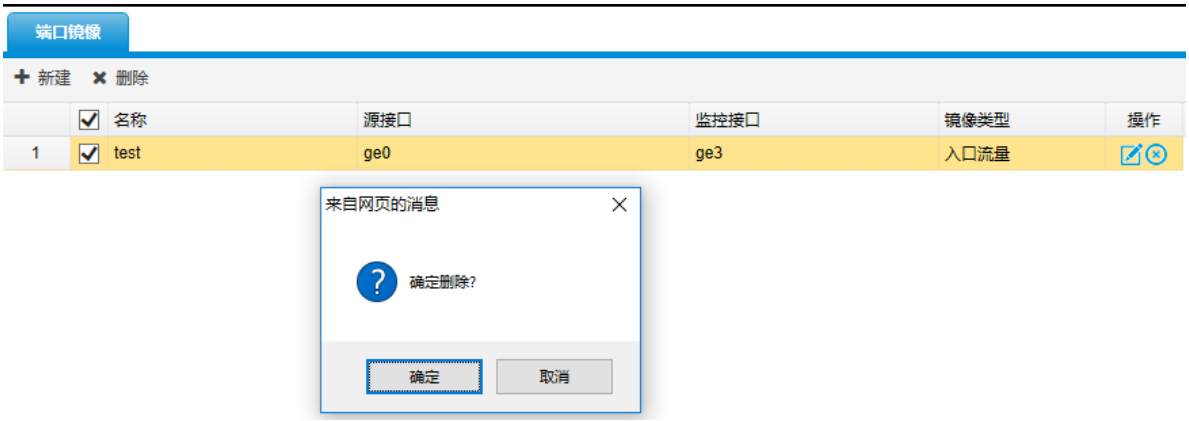
参数	说明
规则类型	根据端口镜像作用的接口模式来划分，分为以下三种类型： 入流量，只对从源接口接收的流量进行镜像。 出流量，只对从源接口发出的流量进行镜像。 双向流量，对源接口接受和发出的双向流量进行镜像。

1.2.3 删除端口镜像规则

1. 单个端口镜像规则删除

通过菜单“网络配置>基础网络>端口镜像”，单击所要删除规则操作中的“删除”按钮，如图 1-3 所示，单击“删除”按钮后再弹出的确认框中选择“确认”按钮进行规则的删除。

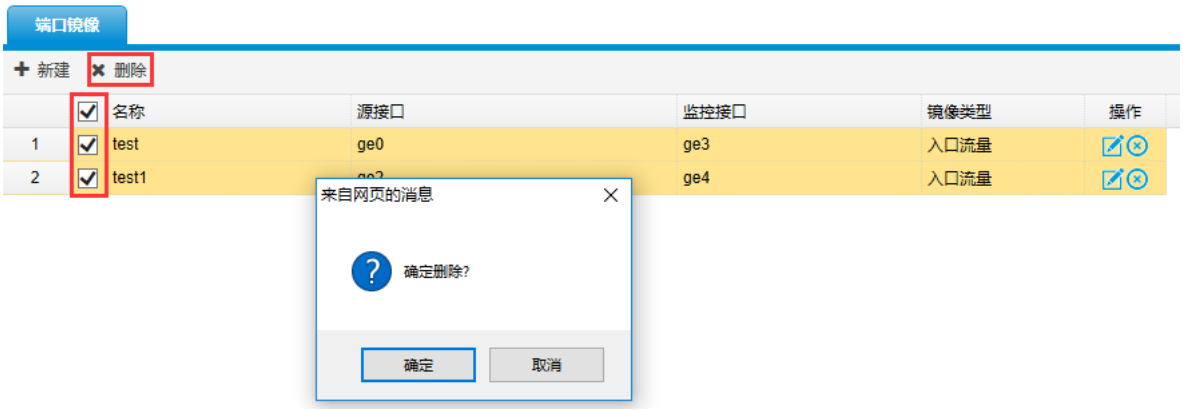
图1-3 单个删除端口镜像规则



2. 批量删除端口镜像规则

通过菜单“网络配置>基础网络>端口镜像”，单击界面上方的“删除”按钮，如图 1-4 所示，单击“删除”按钮后在弹出确认框中选择“确认”按钮进行端口规则的删除。

图1-4 批量删除端口镜像规则配置

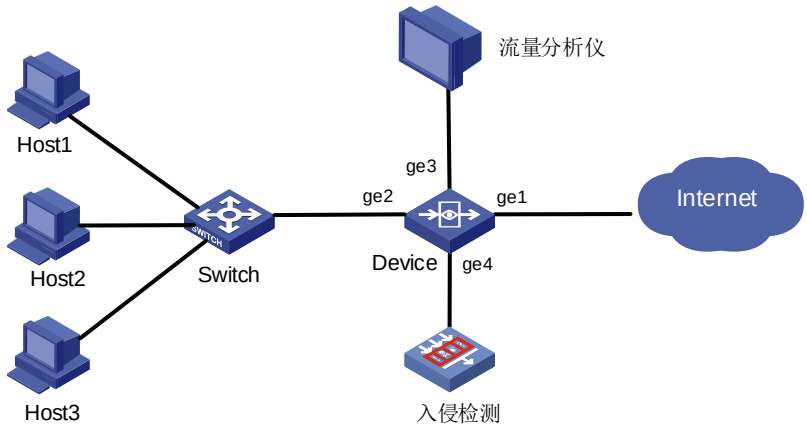


1.3 端口镜像典型配置举例

1.3.1 组网需求

用户两台监控分析设备，功能不同，一台是专用流量分析仪，另一台是入侵检测系统，用户希望能对设备上来回 internet 的流量同时进行流量综合分析和入侵检测，组网如图 1-5 所示。

图1-5 组网图



1.3.2 配置步骤

新建端口镜像规则 test1，源端口为 ge1，监控接口为 ge3，规则类型为双向流量，单击“提交”按钮，如图 1-6 所示。

图1-6 新建端口镜像规则

新建端口镜像规则 test2，源端口为 ge1，监控接口为 ge4，规则类型为双向流量，单击“提交”按钮，如图 1-7 所示。

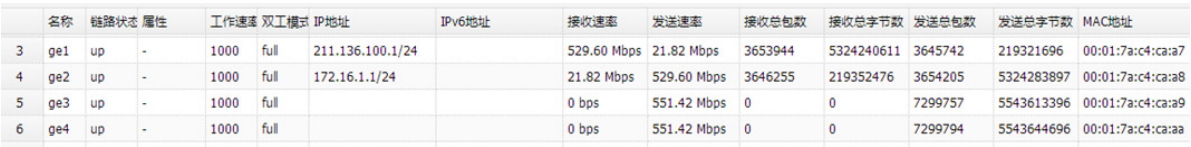
图1-7 新建端口镜像规则

图1-8 配置完成后端口镜像列表

1.3.3 验证配置

在设备查看接口流量大小，如图 1-9 所示，ge3、ge4 接口发送的流量大小等于 ge1 接口接收发送流量之和。

图1-9 验证结果



	名称	链路状态	属性	工作速率	双工模式	IP地址	IPv6地址	接收速率	发送速率	接收总包数	接收总字节数	发送总包数	发送总字节数	MAC地址
3	ge1	up	-	1000	full	211.136.100.1/24		529.60 Mbps	21.82 Mbps	3653944	5324240611	3645742	219321696	00:01:7a:c4:ca:a7
4	ge2	up	-	1000	full	172.16.1.1/24		21.82 Mbps	529.60 Mbps	3646255	219352476	3654205	5324283897	00:01:7a:c4:ca:a8
5	ge3	up	-	1000	full			0 bps	551.42 Mbps	0	0	7299757	5543613396	00:01:7a:c4:ca:a9
6	ge4	up	-	1000	full			0 bps	551.42 Mbps	0	0	7299794	5543644696	00:01:7a:c4:ca:aa

用户在两台监控分析设备上可以同时受到来回 internet 的流量，镜像功能生效，用户可以对来回 internet 流量分别进行综合分析和入侵检测。

目 录

1 部署方式 ····· 1-1
1.1 旁路部署 ····· 1-1
1.2 旁路认证和阻断 ····· 1-1
1.2.1 旁路认证和阻断概述 ····· 1-1
1.2.2 配置旁路认证和阻断 ····· 1-2
1.3 旁路认证和阻断配置举例 ····· 1-2
1.3.1 组网需求 ····· 1-2
1.3.2 配置思路 ····· 1-3
1.3.3 配置步骤 ····· 1-3
1.3.4 配置注意事项 ····· 1-6
1.3.5 验证配置 ····· 1-6

1 部署方式

1.1 旁路部署

通过菜单“网络管理 > 基础网络 > 部署方式”，进入如图 1-1 所示页面。各个配置项的含义如表 1-1 所示。

启用接口旁路部署方式只对报文进行监听，不进行转发。

图1-1 旁路部署页面

表1-1 旁路部署各配置项和显示项含义表

标题项	说明
接口名称	当前系统所有的接口名称。
状态	当前系统部署状态，绿色对号图标为该接口是旁路口。
启用	勾选接口启用，代表该接口启用旁路口。

1.2 旁路认证和阻断

1.2.1 旁路认证和阻断概述

设备旁路部署时支持认证和阻断功能。旁路模式并不替换用户的路由器，也不提供任何 NAT、DHCP 或者 DNS 服务。通常部署在交换机旁边，通过镜像的方式，仅仅提供认证和阻断的功能。旁路模式不修改网络结构，不关心网络细节，关机也不掉线。

适用一些密度高度集中的场所，如大型展会，大型推销活动，演唱会，火车站或者运动会等。

- 对于没有认证的用户发送 http 302 报文重定向。
- 控制策略为拒绝时，对匹配到安全策略的 TCP 报文发送 reset 报文，阻止用户访问网络。

1.2.2 配置旁路认证和阻断

通过菜单“网络管理 > 基础网络 > 部署方式 > 高级配置”，进入如图 1-2 所示页面。在该页面上可以配置旁路认证和阻断相关功能。各个配置项含义如表 1-2 所示。

图1-2 旁路认证配置页面

表1-2 旁路认证和阻断配置项含义表

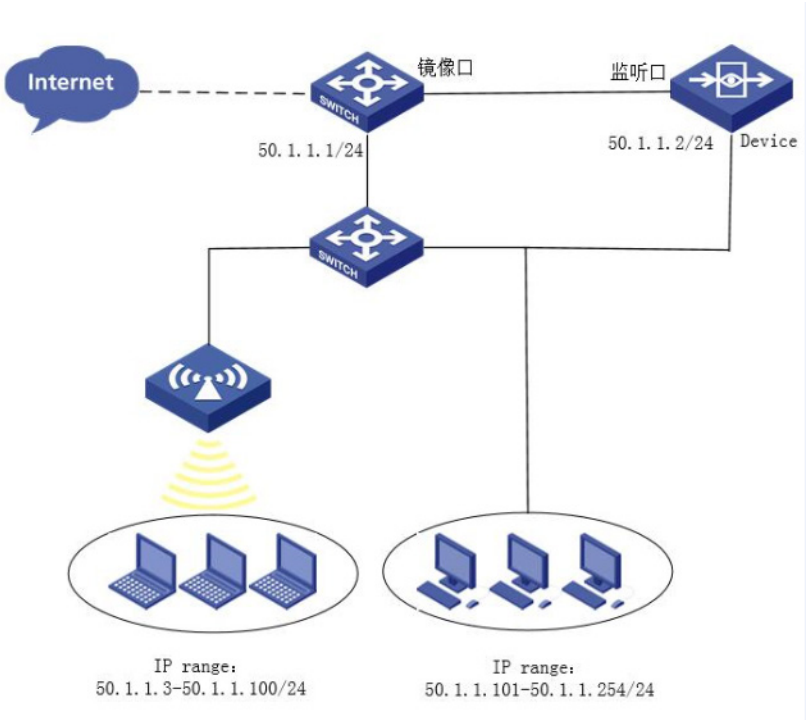
标题项	说明
旁路阻断	旁路阻断开关，开启旁路阻断配合IPV4控制实现旁路阻断功能，默认为关闭。
旁路认证	旁路认证开关，开启旁路认证配合用户认证实现旁路认证功能，默认为关闭。

1.3 旁路认证和阻断配置举例

1.3.1 组网需求

如图 1-3 所示，某企业对内网用户 50.1.1.3-100/24 工作时间都将进行用户认证和内网用户和 50.1.1.101-254/24 工作时间都进行行为控制，不提供任何 NAT，DHCP 或者 DNS 服务。部署在交换机旁边，通过镜像的方式，仅仅提供认证和阻断的功能。旁路模式不修改网络结构，不关心网络细节，关机也不掉线，不会影响企业内部网络。

图1-3 旁路认证和阻断组网图



1.3.2 配置思路

- 配置设备接口地址。
- 配置设备旁路部署。
- 配置设备旁路认证。
- 配置设备旁路阻断。
- 配置用户识别范围。
- 配置用户认证策略。
- 配置 IPv4 控制策略。

1.3.3 配置步骤

(1) 配置接口地址

如图 1-4 所示，进入“网络配置 > 接口配置 > 物理接口”，点击 ge6<编辑>按钮，配置 ge6 的 IP 地址为 50.1.1.2/24。

图1-4 配置接口地址

	接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1	ge0				00:21:45:c8:15:c0	route	full	1000	down		
2	ge1				00:21:45:c8:15:c1	route	full	1000	down		
3	ge2				00:21:45:c8:15:c2	route	full	1000	down		
4	ge3				00:21:45:c8:15:c3	route	full	1000	down		
5	ge4				00:21:45:c8:15:c4	route	full	1000	down		
6	ge5				00:21:45:c8:15:c5	route	full	1000	down		
7	ge6		50.1.1.2/24		00:21:45:c8:15:c6	route	full	1000	up		
8	ge7				00:21:45:c8:15:c7	route	full	1000	down		
9	ge8				00:21:45:c8:15:c8	listen	full	1000	up		
10	ge9				00:21:45:c8:15:c9	route	full	1000	down		

(2) 配置部署方式

如图 1-5 所示，进入“网络管理 > 基础网络 > 部署方式”，配置勾选 ge8 口启用。

图1-5 配置部署方式

	接口名称	状态	启用
1	ge0		
2	ge1		
3	ge2		
4	ge3		
5	ge4		
6	ge5		
7	ge6		
8	ge7		
9	ge8		
10	ge9		

(3) 配置旁路认证和阻断

如图 1-6 所示，进入“网络管理 > 基础网络 > 部署方式 > 高级配置”，配置旁路认证和旁路阻断。

图1-6 配置旁路认证和旁路阻断

(4) 配置内网用户地址对象

如图 1-7 所示，进入“策略配置 > 对象管理 > 地址对象 > IPv4 地址对象”，点击<新建>按钮创建内用户地址对象 50.1.1.0/24、50.1.1.3 和 50.1.1.101，点击<提交>。

图1-7 配置内网用户地址对象

(5) 配置用户识别范围

如图 1-8 所示，进入“用户管理 > 认证管理 > 高级选项 > 全局配置”页面，识别范围选择“50.1.1.0”，其它配置默认，提交配置。

图1-8 用户识别范围

(6) 配置用户认证策略

如图 1-9 所示，进入“用户管理 > 认证管理 > 认证策略”，新建一条认证方式为本地认证的认证策略，源地址选择 50.1.1.3，其它配置默认，<提交>策略。

图1-9 配置用户认证策略

(7) 配置控制策略

如图 1-10 所示，进入“策略配置 > 控制策略”，源地址选择 50.1.1.101，行为选择拒绝，其它配置默认，<提交>策略。

图1-10 配置控制策略

1.3.4 配置注意事项

- 用户认证策略和 IPv4 策略的源接口以及目的接口必须配置接收镜像流量的旁路部署接口或者是 any。
- 旁路认证和阻断务必保证旁路设备到上网 PC 可达，否则功能无法使用。
- 旁路阻断只针对于 TCP 报文生效，对于 UDP、ICMP 等报文无法进行阻断。
- 旁路认证只支持 HTTP 流量触发弹 portal 页面，不支持 HTTPS 流量触发，对 HTTPS 报文直接发送 TCP reset 报文进行阻断。

1.3.5 验证配置

如图 1-11 所示， 内网用户（50.1.1.3）访问外网需要进行本地认证，本地认证成功后，访问外网成功。

图1-11 内网用户需要进行本地认证

如图 1-12 所示，内网用户（50.1.1.101）访问外网资源会被阻断。

图1-12 内网用户访问外网阻断

目 录

1 VRF 配置 1-1
1.1 VRF 简介 1-1
1.2 VRF 显示 1-1
1.3 VRF 添加 1-1
1.4 VRF 编辑 1-2
1.5 VRF 删除 1-2
1.6 VRF 配置举例 1-2
1.6.1 组网需求 1-2
1.6.2 配置步骤 1-2

1 VRF 配置

1.1 VRF简介

VRF：Virtual Routing Forwarding，VPN 路由转发表，是一项计算机网络技术，它允许一个路由表的多个实例在同一时间同一个路由器共存。因为它的路由实例是独立的，可以使用相同的或者重叠的 IP 地址而不会产生冲突。VRF 功能提供了从一台物理路由器变成多台虚拟路由器的功能。

1.2 VRF显示

通过菜单“网络配置 > 基础网络 > VRF 配置”，进入到 VRF 显示界面，如图 1-1 所示。

图1-1 VRF 显示界面

1.3 VRF添加

通过菜单“网络配置 > 基础网络 > VRF 配置”，进入到如图 1-1 所示 VRF 显示界面。点击<新建>按钮，页面切换到 VRF 新建页面，如图 1-2 所示。

图1-2 VRF 新建界面

表1-1 VRF 配置说明

配置项	说明
VRF名称	要创建的VRF名称
接口列表	左侧框内为可以加入这个VRF的接口的列表 右侧框内为已经加入该VRF的接口的列表

1.4 VRF编辑

通过菜单“网络配置 > 基础网络 > VRF 配置”，进入到如图 1-1 所示 VRF 显示界面。点击<编辑>按钮，页面切换到 VRF 编辑页面，如图 1-3 所示，可以修改加入该 VRF 的接口。

图1-3 VRF 编辑页面

1.5 VRF删除

通过菜单“网络配置 > 基础网络 > VRF 配置”，进入到如图 1-1 所示 VRF 显示界面。点击要删除的 VRF 对应的<删除>按钮，删除该 VRF。

1.6 VRF配置举例

1.6.1 组网需求

添加一个名为 test2，包含有 ge4，ge5 两个接口的 VRF。

1.6.2 配置步骤

(1) 进入 VRF 的显示界面，点击<新建>按钮。

图1-4 VRF 显示界面

(2) 在弹出的新建页面中配置 VRF。

图1-5 VRF 新建页面

(3) 点击<提交>按钮，可以在 VRF 显示页面中看到我们配置的 test2.

图1-6 VRF 显示界面

目 录

1 用户管理 ····· 1-1
1.1 概述 ····· 1-1
1.1.1 用户和用户分类 ····· 1-1
1.1.2 用户组织结构以及属性组 ····· 1-1
1.2 用户和用户组配置 ····· 1-1
1.2.1 配置用户或用户组 ····· 1-1
1.2.2 批量编辑用户 ····· 1-8
2 用户认证 ····· 2-9
2.1 配置概述 ····· 2-9
2.2 配置认证服务器 ····· 2-9
2.2.1 配置 LDAP ····· 2-9
2.2.2 配置 RADIUS ····· 2-15
2.2.3 配置 POP3 服务器 ····· 2-17
2.3 认证设置 ····· 2-18
2.3.1 认证模板设置 ····· 2-18
2.3.2 本地 WEB 认证配置 ····· 2-34
2.3.3 微信认证配置 ····· 2-37
2.3.4 短信认证配置 ····· 2-39
2.3.5 Portal Server 认证配置 ····· 2-40
2.3.6 免认证配置 ····· 2-41
2.3.7 访客二维码认证 ····· 2-42
2.3.8 IC 卡认证 ····· 2-44
2.3.9 APP 认证 ····· 2-44
2.3.10 POP3 认证 ····· 2-46
2.3.11 钉钉认证 ····· 2-47
2.3.12 混合认证 ····· 2-49
2.4 第三方用户同步 ····· 2-50
2.4.1 第三方用户同步接口 ····· 2-50
2.4.2 Radius 用户同步 ····· 2-51
2.4.3 web 用户同步（http 流量经过设备） ····· 2-52
2.4.4 web 用户同步（http 流量到达设备） ····· 2-54
2.4.5 其它用户同步 ····· 2-55

2.5 全局配置 ····· 2-56
2.6 用户认证策略 ····· 2-58
2.6.1 用户认证策略概述 ····· 2-58
2.6.2 认证策略配置 ····· 2-58
2.7 配置举例 ····· 2-60
2.7.1 用户认证策略配置举例 ····· 2-60
2.7.2 LDAP 使用标识名 CN 认证典型配置举例 ····· 2-72
2.7.3 LDAP 使用标识名 sAMAccountName 认证典型配置案例 ····· 2-76
2.7.4 LDAP 控制认证用户名是否区分大小写配置举例 ····· 2-80
2.7.5 LDAP 使用同步安全组认证配置举例 ····· 2-86

1 用户管理

1.1 概述

1.1.1 用户和用户分类

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。

根据用户的认证状态，可以将用户分为三类：匿名用户、静态绑定用户、认证用户。

- 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，是指系统根据静态配置识别出的用户；系统支持以 CSV 文件的方式，将静态绑定用户批量导入和导出。
- 认证用户，是指根据系统配置，需要进行认证的用户。其中认证方式，支持本地用户数据库、短信认证、微信认证、访客二维码认证、RADIUS 服务器/服务器组、LDAP 服务器/服务器组的用户认证，认证用户所使用的 IP 地址可以是 IPv4 地址也可以是 IPv6 地址。。

根据不同的用户分类，可以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。

1.1.2 用户组织结构以及属性组

通过用户组织结构可以清晰的将每个用户按照组织架构进行分类处理，方便管理和维护。属性组则是为每个用户附加一个或者多个属性，这样可以通过属性组的方式将某一类用户进行管控。

- 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，支持 8 级层级，每个层级支持 1024 个节点。
- 属性组没有层级结构，全部属性组组使用并列的形式。
- 同一用户在组织结构组中仅可出现一次。
- 属性组中相同用户可以同时存在于多个属性组。

1.2 用户和用户组配置

1.2.1 配置用户或用户组

1. 创建用户和用户组

在导航栏中选择“用户管理 > 用户组织结构”，选择用户显示页面，如图 1-1 所示。

图1-1 用户显示页面

页面的详细说明如表 1-1 所示。

表1-1 用户组的详细说明

项目	说明
组织结构	以树形结构的方式展示所有用户的组织结构信息，最大支持8级的组织结构。
名称	该用户组下的用户或者下一级用户组的名称，1-63字符。
描述	用户组或者用户的描述信息，没有则为空。
类型	此行对应的是用户组或用户。
所属用户组	上一级用户组的名称，如果该用户组的所属用户组为“/”，则表示该用户的上一级用户组为根组。
绑定范围	显示该用户绑定的IP或者MAC地址。
状态	该用户是否生效。
引用	该用户在系统中被策略引用的次数。
操作	可以修改或者删除该用户或者用户组，被引用或者预定义的用户和用户组不能被删除。

选择“用户管理 > 用户组织结构”，将鼠标移至<新建>按钮，在下拉框中选择“组”，进入用户组的新建页面，如图 1-2 所示。

图1-2 用户组新建页面

页面的详细说明如表 1-2 所示。

表1-2 用户组新建页面详细说明

项目	说明
名称	用户组的名称。
描述	用户组的描述。
路径	用户组所属的路径。

按照需求输入对应的项目后，单击<提交>，即可将该用户组加入到选择的路径下。

选择“用户管理>用户”，将鼠标移至<新建>按钮，在下拉框中选择“用户”，进入用户的新建页面，如图 1-3 所示。

图1-3 用户新建页面

页面的详细说明如表 1-3 所示。

表1-3 用户新建页面详细说明

项目	说明
启用	用户是否启用。
登录名	用户的名称。
描述	关于用户的描述。
所属组	用户所属于的用户组。
本地密码	勾选之后设置用户的本地密码，不勾选代表此用户为无密码或者为第三方服务器认证用户，密码记录在地三方服务器。
确认密码	重新确认一次密码，防止误操作。
允许修改密码	允许本地认证用户修改登录密码。
初次认证修改密码	强制本地认证用户在第一登录时修改密码。
绑定范围	用户登录的地址范围，支持IPv4/IPv6主机，IPv4/IPv6地址范围，网络和mac地址的绑定。
排除IP	用户登录的地址范围内排除IP，只支持IPv4地址。
账户过期时间	账号有效期，可选择永不过期或者在某天后过期。

点击“高级选项”页签，切换到用户的高级选项配置页面，如下图所示。

图1-4 用户高级配置页面

表1-4 用户高级配置页面详细说明

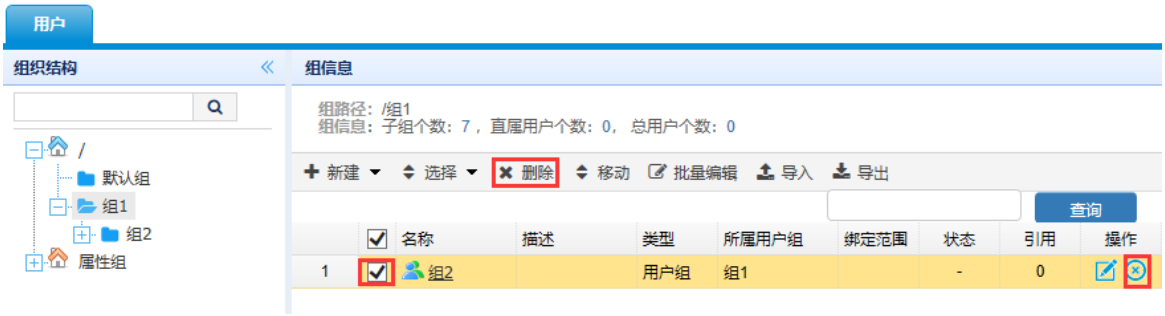
项目	说明
用户登录唯一性检查	是否启用用户唯一性检查的配置方式，勾选为启用。
单一账号登录	同一时间只允许同一账号登录一次。 启用单一账号登录后，可针对已登录用户做如下2种处理方式： • 踢出已登录用户：如果新用户登录，老的用户将会被踢下线； • 禁止同名用户再次登录：如果老用户已经登录，新用户将不能以此用户名登录。
允许重复登录	同一时间允许同一账号登录多次。 启用允许重复登录后，允许个数支持无限制和限制登录个数。
账户过期时间	账号有效期，可选择永不过期或者在某天后过期。

按照需求输入对应的项目后，单击<提交>，即可将该用户加入到选择的用户组下。

2. 删除用户或用户组

在组信息显示页面，勾选中用户或者用户组后，单击列表上方的<删除>按钮，或者单击对应用户或用户组操作中的<删除>按钮，如图 1-5 所示，可以删除对应的用户组或者用户。

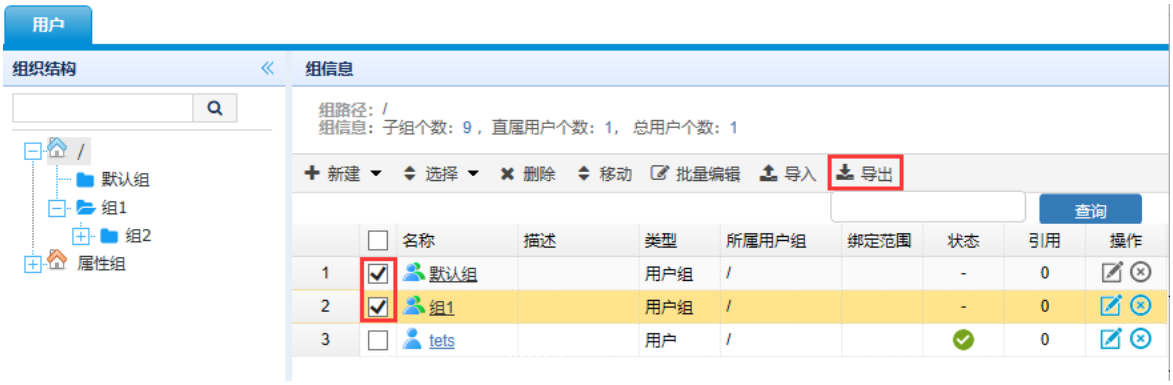
图1-5 删除用户组



3. 导出用户和用户组

在用户显示页面，勾选需要导出的用户和用户组信息，再单击页面上方的<导出>按钮，可以将所选的本地用户和用户组导出成 csv 文件。

图1-6 导出用户组



说明

导出的文件中只包含勾选的用户或者用户组信息，用户组内的用户或者下一级用户组信息不能导出。

4. 导入用户和用户组

在用户显示页面单击<导入>按钮，弹出导入用户弹窗，在弹窗的左下角单击“下载模板”，可以下载用户导入模板，将用户和用户组信息录入模板后，在弹窗的上传文件名称中选择修改后的模板，并勾选需要的选项，单击<提交>按钮即可将用户或者用户组导入到系统中。

图1-7 导入用户组

导入用户的详细说明如所示。

表1-5 导入用户详细说明

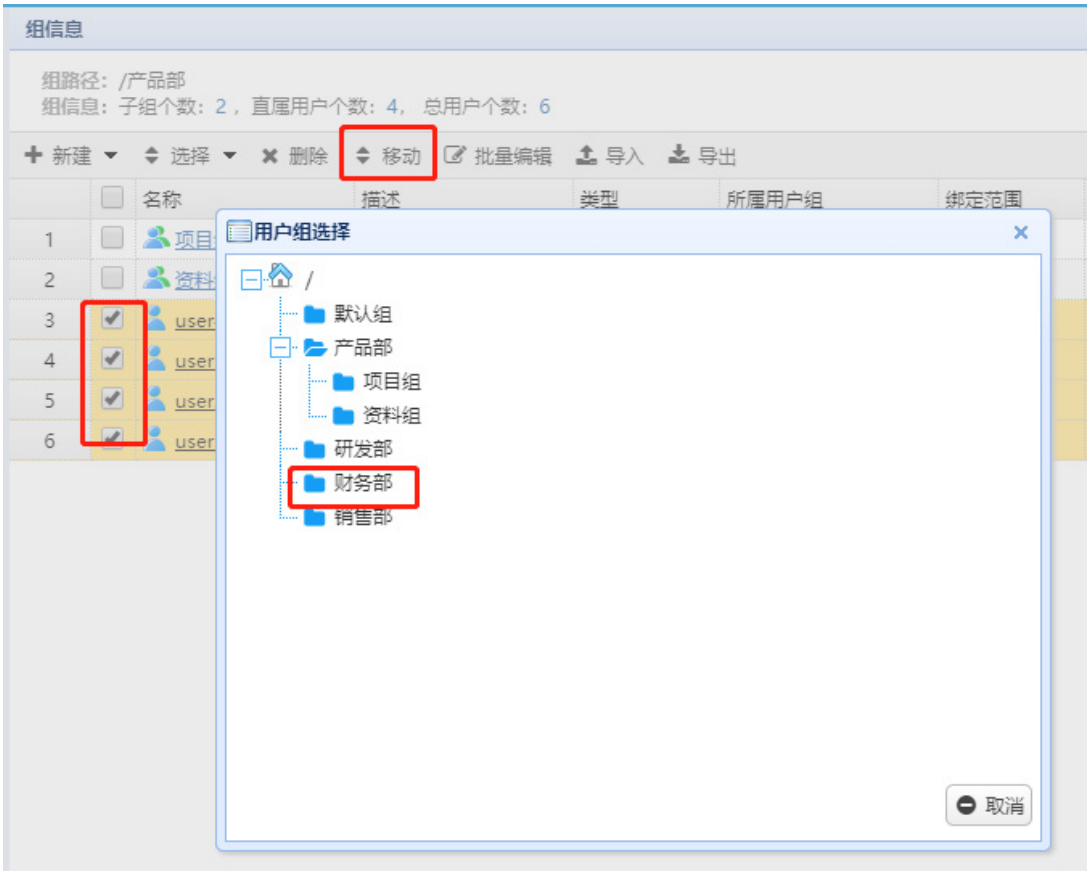
项目	说明
上传文件名称	选择本地已经录入用户的模板文件。
当用户所属组不存在时，自动创建	勾选后，如所填写的所属用户组在本地不存在，则自动创建该用户组。
对本地已经存在的用户	可以选择继续覆盖本地用户或者跳过该用户的导入。
对有本地密码的用户，要求初次登录时修改初始密码	勾选后，有本地密码的用户首次登录时要求修改初始密码。

5. 移动用户和用户组

通过用户和用户组移动功能，可以同时将多个用户或者用户组以及用户组中的子用户组和用户移动到指定的用户组中。

通过菜单“用户管理 > 用户组织结构”，选择勾选需要移动的用户或者用户组（也可以通过选择按钮快捷选择用户和用户组），单击<移动>，在用户组选择弹窗中单击目标用户组，即可将选中的用户和用户组移动到目标用户组中。如图 1-8 所示。

图1-8 用户和用户组移动



1.2.2 批量编辑用户

使用用户批量编辑功能，可以同时对多个用户属性进行编辑。

说明

仅用户支持批量编辑功能，用户组不支持批量编辑。

选择“用户管理>用户组织结构”，进入用户列表，勾选需要批量修改的用户，单击列表上方的<批量编辑>按钮，即可进入批量编辑用户页面。如图 1-9 所示。

图1-9 批量编辑用户

批量编辑用户页面的详细说明如下表所示。

表1-6 批量编辑用户页面说明

标题项	说明
用户	进行批量编辑的用户
用户状态	勾选则修改用户状态，不勾选则不修改用户状态 勾选后，选择启用则选择的用户状态批量修改为启用；选择禁用则批量修改为禁用。
密码设置	选择用户的密码统一重置密码。 勾选允许修改密码则用户允许自行修改密码 勾选初次认证修改密码则用户初次登录是强制修改密码。

2 用户认证

2.1 配置概述

用户认证配置的推荐步骤如表 2-1 所示。

表2-1 用户和用户认证配置的推荐步骤

配置任务	说明	详细配置
配置用户和用户组	必选	1.2
配置认证服务器	可选（使用第三方认证服务器时选择。）	2.2
第三方用户同步	可选（使用第三方认证服务器时选择。）	2.4
配置高级选项	必选	2.5
配置认证设置	必选	2.3
配置认证策略	可选	2.6

2.2 配置认证服务器

本小节中的认证服务器是指第三方的 Radius 或者 LDAP 认证服务器，主要用于第三方用户同步和认证。

2.2.1 配置 LDAP

1. LDAP 简介

LDAP 是轻量目录访问协议，英文全称是 lightweight Directory Access Protocol，一般都简称为 LDAP。它是基于 X.500 标准的，与 X.500 不同，LDAP 支持 TCP/IP。

LDAP 是一个用来发布目录信息到许多不同资源的协议。通常它都作为一个集中的地址本使用，LDAP 其实是一电话簿，类似于我们所使用诸如 NIS(Network Information Service)、DNS (Domain Name Service)等网络目录，也类似于你在花园中所看到的树木。

在一些存在众多分支机构的大企业等网络中，往往存在 LDAP（轻量级目录访问协议）系统，用户信息都由 LDAP 系统进行管理，如果分支机构间的人员出差频繁而又不符合漫游策略，为方便管理员开户操作，可以从 LDAP 系统中同步用户信息。

通过 LDAP 同步将 AD 服务器上的用户及用户组同步到设备上，对同步下来的用户及用户组可进行引用和策略管控，具体请参考“用户同步”章节。

同步方式为周期同步和触发同步两种：

- 设备周期向 AD 服务器发送 LDAP 同步请求。
- 可通过界面手动发起 LDAP 同步请求。

2. 使用限制及注意事项

- 无论直接使用 LDAP 服务器进行第三方认证，还是通过 LDAP 同步将 AD 服务器上的用户同步到本地做本地认证，用户的账号、密码都是通过 LDAP 服务器进行校验。
- LDAP 同步成功后，可以将 AD 服务器上的用户账号及用户所属组织结构同步到本地设备，以实现对用户的引用和策略管控。
- 如需对 LDAP 同步后的用户进行策略管控，配置 LDAP 同步后，还需配置本地认证功能，同步后的用户通过认证上线后，在相关策略被引用才会生效。

3. 配置 LDAP 服务器

在导航栏中选择“用户管理>认证管理>认证服务器”，进入认证服务器配置页面，将鼠标移至<新建>按钮，在下拉框中选择“LDAP 服务器”，进入 LDAP 服务器的配置界面，如图 2-1 所示。LDAP 服务器详细参数如表 2-2 所示。

图2-1 LDAP 服务器配置界面

表2-2 LDAP 服务器界面的详细说明

参数	说明
服务器名称	LDAP服务器名称。
服务器IP	LDAP服务器地址。
端口	LDAP服务器端口，默认389明文，暂时不支持636加密同步。
通用标识	cn：全称 common name，配置cn时，同步、认证都使用标识名。 sAMAccountName：同步和认证使用登录名。
Base DN	用于获取同步信息的服务器域名路径。
管理员	拥有管理权限的域服务器管理员。
管理员密码	管理员对应密码。

4. 配置 LDAP 组

在导航栏中选择“用户管理>认证管理>认证服务器>服务器组”，将鼠标移至<新建>按钮，在下拉框中选择“LDAP 组”，进入 LDAP 组配置界面，如图 2-2 所示。LDAP 组详细参数如表 2-3 所示。

图2-2 LDAP 组新建界面

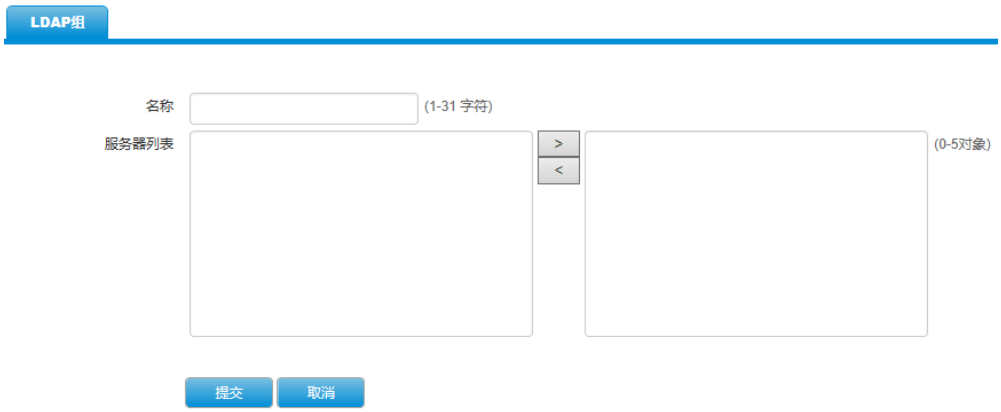


表2-3 LDAP 组界面的详细说明

参数	说明
名称	LDAP组名称。
服务器列表	已配置的LDAP服务器名称，最多可加入5个服务器。

5. LDAP 组用法

在“用户管理>认证管理>高级选项>全局配置>认证配置”处，选择 LDAP 组统一认证。

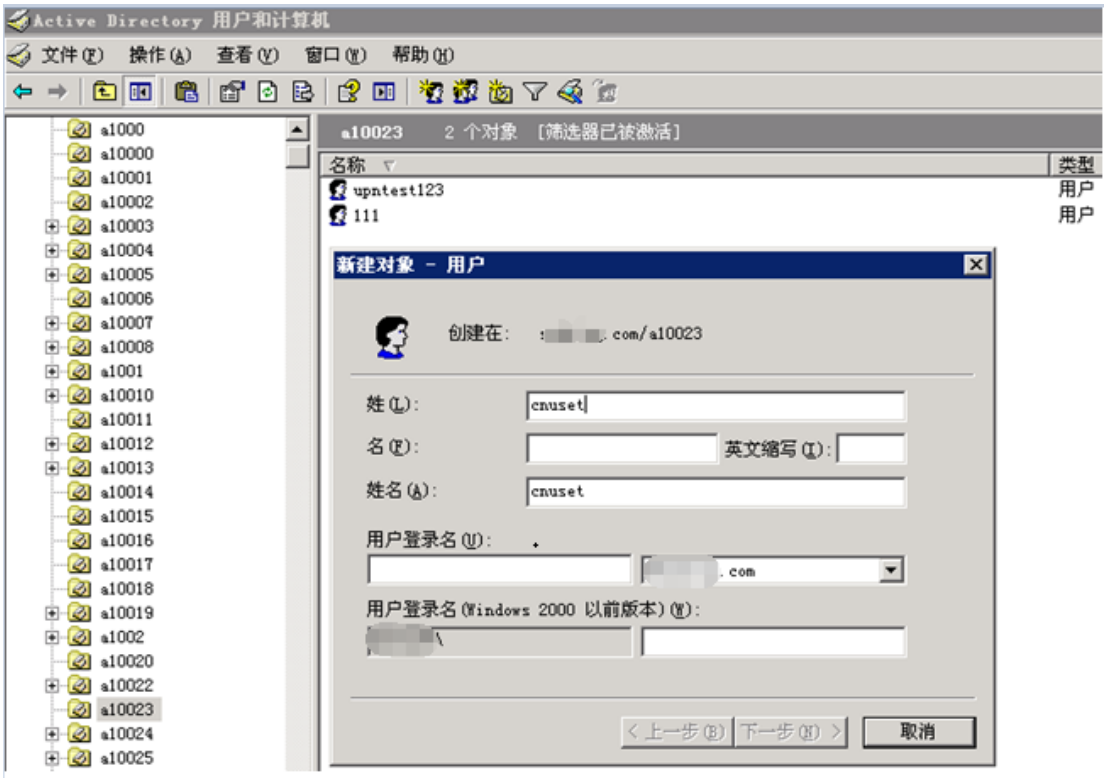
6. LDAP 认证的两种方式

LDAP 用户认证通用名标识有两种类型分别是 CN 和 sAMAccountName，如图 2-3 所示。

图2-3 LDAP 用户认证通用名标识类型

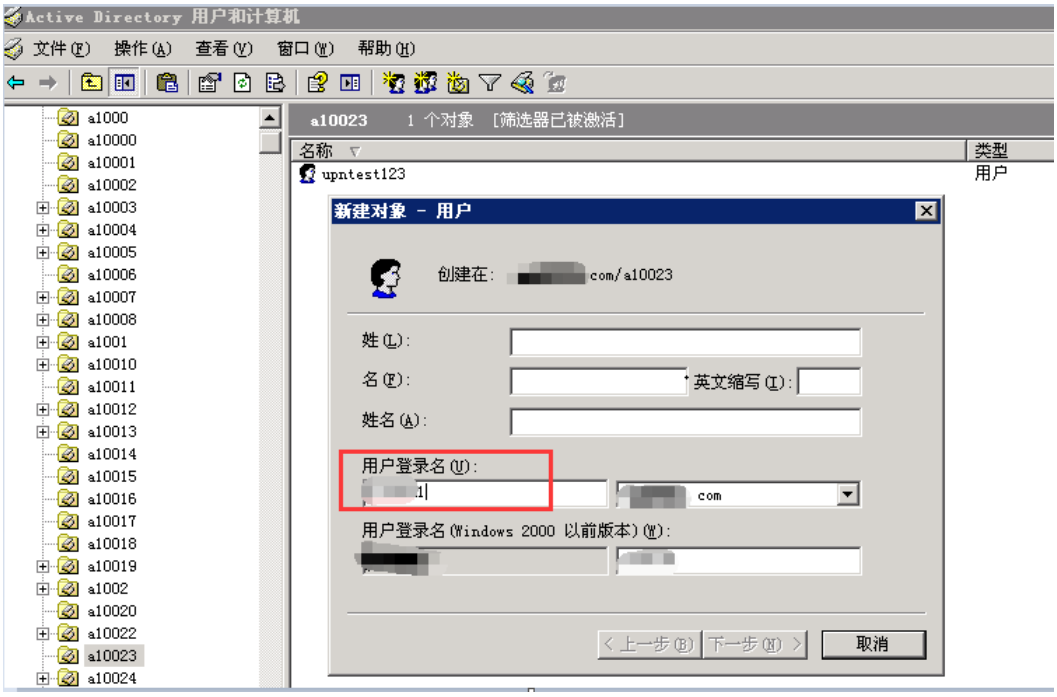
CN：使用的是标识名进行认证，标识名使用 CN 时服务器用户配置如图 2-4 所示。

图2-4 标识名使用 CN 时服务器用户配置



sAMAccountName：使用的是登录名进行认证，标识名使用 sAMAcountName 时服务器用户配置如图 2-5 所示。

图2-5 标识名使用 sAMAcountName 时服务器用户配置



2.2.2 配置 RADIUS

1. 配置 RADIUS 服务器

在导航栏中选择“用户管理>认证管理>认证服务器”，将鼠标移至<新建>按钮，在下拉框中选择“RADIUS 服务器”，进入 RADIUS 服务器的配置界面，如图 2-6 所示。RADIUS 服务器详细参数如表 2-4 所示。

图2-6 RADIUS 服务器配置页面

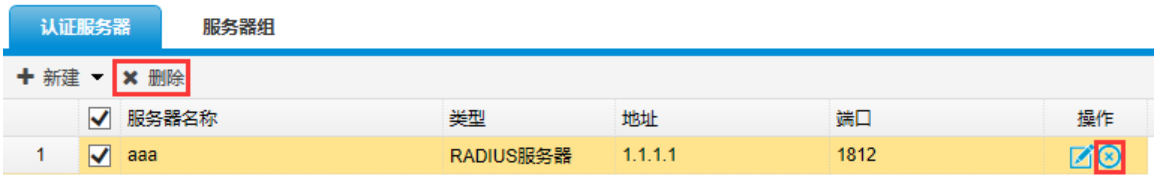
表2-4 RADIUS 服务器创建页面详细说明

项目	说明
服务器名称	RADIUS服务器名称。
服务器地址	RADIUS服务器地址。
服务器密码	RADIUS服务器密码。
端口	RADIUS服务器端口，缺省为1812。
认证方式	可以选择pap或chap两种认证方式，chap比pap认证方式更安全，建议选择chap。

输入完毕后，点击<提交>按钮，应用配置。

在认证服务器显示页面，选中 RADIUS 服务器后，点击页面上上方的<删除>按钮，或者点击对应 RADIUS 服务器的<删除>按钮，如图 2-7 所示，可以删除对应的 RADIUS 服务器。

图2-7 删除 RADIUS 服务器



2. RADIUS 组配置

在导航栏中选择“用户管理>认证管理>认证服务器>服务器组”，将鼠标移至<新建>按钮，在下拉框中选择“RADIUS 组”，进入 RADIUS 组配置界面，如图 2-8 所示。RADIUS 组详细参数如表 2-5 所示。

图2-8 RADIUS 服务器组配置页面

表2-5 RADIUS 服务器组创建页面详细说明

项目	说明
名称	RADIUS服务器组名称。
服务器列表	已经配置的RADIUS服务器列表。

选中左边的服务器列表中的服务器，点击<添加>按钮，可以将选中服务器添加到服务器组中。

选中右边的服务器列表中的服务器，点击<删除>按钮，可以将选中服务器从服务器组中删除。

输入完毕后，点击<提交>按钮，应用配置。

在 RADIUS 服务器组显示页面，点击对应 RADIUS 服务器组的<删除>按钮，可以删除对应的 RADIUS 服务器。

2.2.3 配置 POP3 服务器

1. 配置 POP3 服务器

在导航栏中选择“用户管理 > 认证管理 > 认证服务器”，进入认证服务器界面。将鼠标移至“新建”按钮，在下拉框中选择“POP3 服务器”，进入 POP3 服务器的配置界面，如下图所示。

图2-9 POP3 服务器配置界面

表2-6 POP3 服务器界面的详细说明

参数	说明
服务器名称	设备上用来唯一标识POP3服务器的名称，与POP3服务器本身的名称无关，可以相同也可以不同。
服务器地址	POP3服务器地址。输入提供认证服务的POP3服务器的IP地址。
服务器端口	POP3服务器端口，缺省为995。
SSL	可以选择勾选SSL加密和不勾选SSL加密。默认勾选SSL加密方式，勾选SSL加密方式提高安全性，防止用户名和密码在传输中泄漏。

1. 配置 POP3 服务器组

在导航栏中选择“用户管理 > 认证管理 > 认证服务器 > 服务器组”，将鼠标移至“新建”按钮，在下拉框中选择“POP3 组”，进入 POP3 组配置界面，如下图所示。

图2-10 POP3 服务器组新建界面

表2-7 POP3 服务器组界面的详细说明

参数	说明
名称	POP3服务器组名称。
服务器列表	已经配置的POP3服务器列表。

选中左边的服务器列表中的服务器，单击“添加”按钮，可以将选中服务器添加到服务器组中；选中右边的服务器列表中的服务器，单击“删除”按钮，可以将选中服务器从服务器组中删除。

2.3 认证设置

2.3.1 认证模板设置

1. 认证模板设置

在导航栏中选择“用户管理>认证管理>认证方式>认证模板设置”，进入认证模板显示页面，页面显示了当前所有认证模板的类型，如图 2-11 所示。

图2-11 认证模板设置页面

表2-8 认证模板设置页面详细说明

项目	说明
名称	认证模板名称，不支持编辑。
描述	认证模板描述，不支持编辑。
预览	模板设置完成后支持PC端和移动端效果预览。
操作	对模板进行编辑、重置等操作。

2. 本地认证模板

在导航栏中选择“用户管理>认证管理>认证方式>认证模板设置>本地认证模板”，点击操作中的<编辑>按钮进入本地认证模板配置页面，页面显示了当前的本地认证模板配置，如图 2-12 所示。

图2-12 本地认证模板配置页面

页面的详细说明如表 2-9 所示。

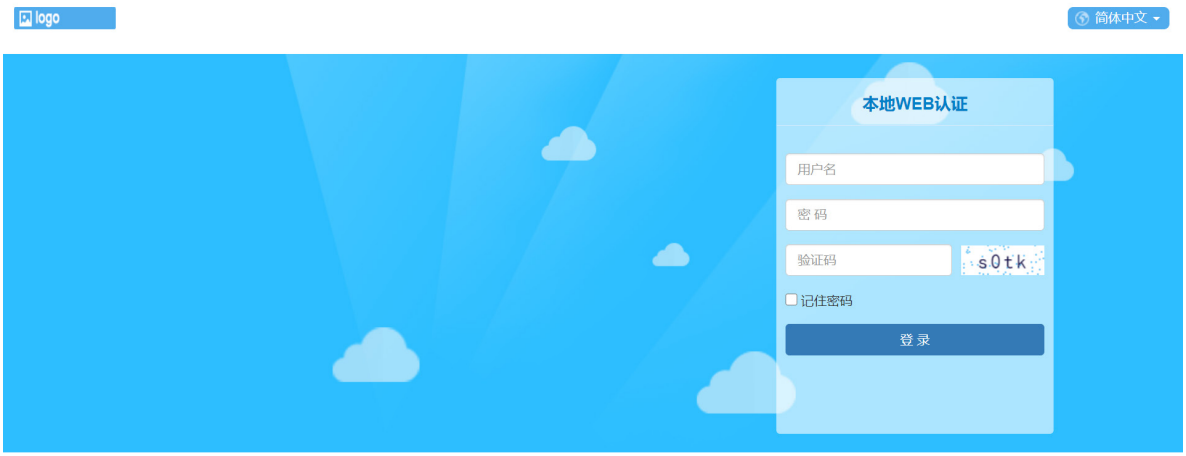
表2-9 本地认证模板配置详细说明

项目	说明
标签页名称	本地认证Portal页面显示的标签名称。
欢迎词	本地认证模板欢迎词。
免责声明	本地认证模板免责声明。
按钮颜色	登录按钮颜色。
Logo图片	Logo图片设置 。
背景图片	本地认证Portal页面背景图片。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

点击预览图标查看 PC 终端预览效果，如图 2-13 所示。

图2-13 本地认证模板 PC 终端预览效果



点击预览图标查看移动终端预览效果，如图 2-14 所示

图2-14 本地认证模板移动终端预览效果

3. 微信认证模板

在导航栏中选择“用户管理>认证管理>认证方式>认证模板设置>微信认证模板”，点击操作中的<编辑>按钮进入微信认证模板配置页面，页面显示了当前的微信认证模板配置，如图 2-15 所示。

图2-15 微信认证模板配置页面

页面的详细说明如表 2-10 所示。

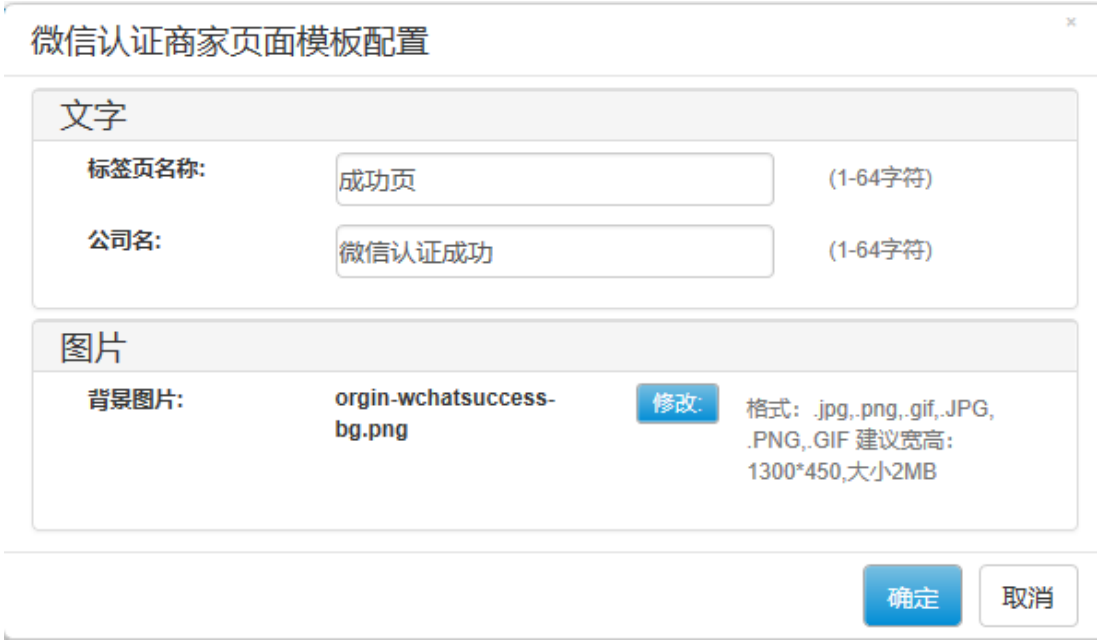
表2-10 微信认证模板配置详细说明

项目	说明
标签页名称	微信认证Portal页面显示的标签名称。
欢迎词	微信认证模板欢迎词。
免责声明	微信认证模板免责声明。
Logo图片	Logo图片设置 。
背景图片	微信认证Portal页面背景图片。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

点击操作中的<成功页面编辑>按钮进入微信认证商家页面模板配置，页面显示了当前的微信认证商家页面模板配置，如图 2-16 所示。

图2-16 微信认证商家页面模板配置



页面详细说明如表 1-4 所示。

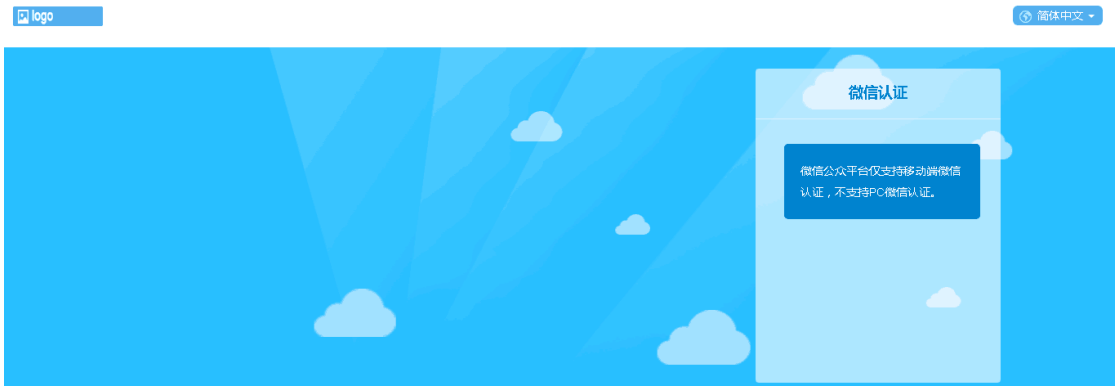
表2-11 微信认证商家页面模板配置详细说明

项目	说明
标签页名称	微信认证Portal页面显示的标签名称。
欢迎词	认证后的欢迎词。
背景图片	微信认证显示成功后页面的背景图片。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

点击预览图标查看 PC 终端预览效果，如图 2-17 所示。

图2-17 微信认证模板 PC 终端预览效果



说明

目前微信公众平台仅支持移动端微信认证，不支持 PC 端微信认证。

点击预览图标查看移动终端预览效果，如图 2-18 所示

图2-18 微信认证模板移动终端预览效果

4. 短信认证模板

在导航栏中选择“用户管理>认证管理>认证方式>认证模板设置>短信认证模板”，点击操作中的<编辑>按钮进入短信认证模板配置页面，页面显示了当前的短信认证模板配置，如图 2-19 所示。

图2-19 短信认证模板配置页面

页面的详细说明如表 2-12 所示。

表2-12 短信认证模板配置详细说明

项目	说明
标签页名称	短信认证Portal页面显示的标签名称。
欢迎词	短信认证模板欢迎词。
免责声明	短信认证模板免责声明。
发送按钮颜色	发送短信验证码按钮颜色。
登录按钮颜色	点击认证登录按钮颜色。
Logo图片	Logo图片设置 。
背景图片	短信认证Portal页面背景图片。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

点击预览图标查看 PC 终端预览效果，如图 2-20 所示。

图2-20 短信认证模板 PC 终端预览效果

点击预览图标查看移动终端预览效果，如图 2-21 所示

图2-21 短信认证模板移动终端预览效果

5. 免认证模板

在导航栏中选择“用户管理>认证管理>认证方式>认证模板设置>免认证模板”，点击操作中的<编辑>按钮进入免认证模板配置页面，页面显示了当前的免认证模板配置，如图 2-22 所示。

图2-22 免认证模板配置页面

页面的详细说明如表 2-13 所示。

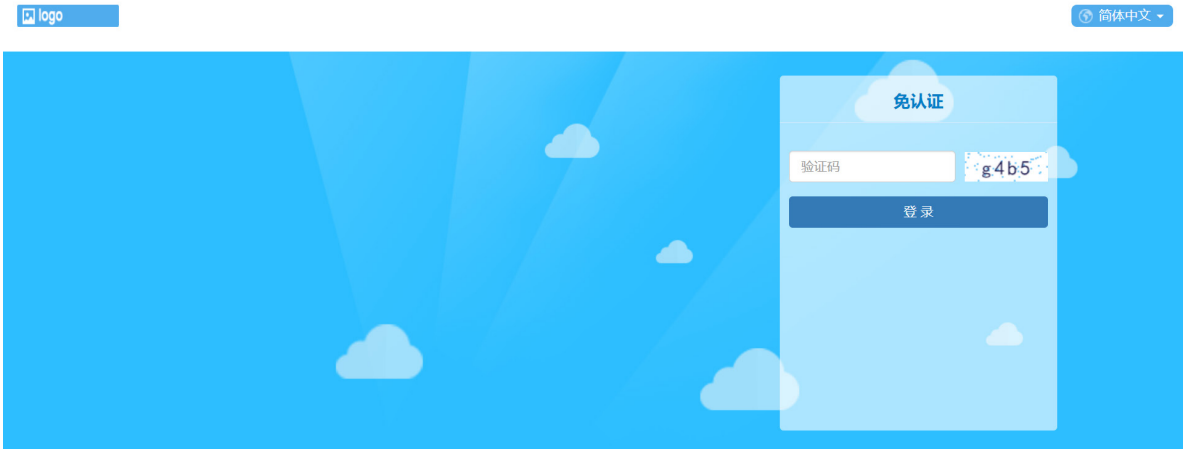
表2-13 免认证模板配置详细说明

项目	说明
标签页名称	免认证Portal页面显示的标签名称。
欢迎词	免认证模板欢迎词。
免责声明	免认证模板免责声明。
免认证描述	免认证portal页面显示的描述信息。
按钮颜色	免认证登录按钮颜色。
Logo图片	免认证模板Logo图片 。
背景图片	免认证Portal页面背景图片。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

点击预览图标查看 PC 终端预览效果，如图 2-23 所示。

图2-23 免认证模板 PC 终端预览效果



点击预览图标查看移动终端预览效果，如图 2-24 所示

图2-24 免认证模板移动终端预览效果

6. 二维码认证模板

在导航栏中选择“用户管理>认证管理>认证方式>认证模板设置>二维码认证模板”，点击操作中的<编辑>按钮进入二维码认证模板配置页面，页面显示了当前的二维码认证模板配置，如图 2-25 所示。

图2-25 二维码认证模板配置页面

页面的详细说明如表 2-14 所示。

表2-14 二维码认证模板配置详细说明

项目	说明
标签页名称	二维码认证Portal页面显示的标签名称。
欢迎词	二维码认证模板欢迎词。
免责声明	二维码认证免责声明。
按钮颜色	登录按钮颜色。
Logo图片	Logo图片设置 。
背景图片	二维码认证Portal页面背景图片。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

点击预览 图标查看 PC 终端预览效果，如图 2-26 所示。

图2-26 二维码认证模板 PC 终端预览效果

点击预览图标查看移动终端预览效果，如图 2-27 所示。

图2-27 二维码认证模板移动终端预览效果

7. 钉钉认证模板

在导航栏中选择“用户管理>认证管理>认证方式>认证模板设置>钉钉认证模板”，点击操作中的<编辑>按钮进入钉钉认证模板配置页面，页面显示了当前的钉钉认证模板配置，如下图所示。

图2-28 钉钉认证模板配置页面

页面的详细说明如表 2-17 所示。

表2-15 钉钉认证模板配置详细说明

项目	说明
标签页名称	钉钉认证Portal页面显示的标签名称。
欢迎词	钉钉认证模板欢迎词。
免责声明	钉钉认证模板免责声明。
Logo图片	Logo图片设置 。
背景图片	钉钉认证Portal页面背景图片。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

点击预览图标查看 PC 终端预览效果，如下图所示。

图2-29 钉钉认证模板 PC 终端预览效果

点击预览图标查看移动终端预览效果，如下图所示。

图2-30 钉钉认证模板移动终端预览效果

8. 混合认证模板

在导航栏中选择“用户管理>认证管理>认证方式>认证模板设置>混合认证模板”，点击操作中的<编辑>按钮进入混合认证模板配置页面，页面显示了当前的混合认证模板配置，如图 2-31 所示。

图2-31 混合认证模板配置页面

页面的详细说明如表 2-16 所示。

表2-16 混合认证模板基本配置详细说明

项目	说明
标签页名称	混合认证模板Portal页面显示的标签名称。
欢迎词	混合认证模板欢迎词。
免责声明	混合认证模板免责声明。
登录按钮颜色	混合认证模板登录按钮颜色。
Logo图片	Logo图片设置 。
背景图片	混合认证模板Portal页面背景图片，同时支持3张背景图片混合认证显示。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

点击操作中的<高级配置>按钮进入混合认证模板高级配置，页面显示了当前的混合认证模板高级配置，如图 2-32 所示。

图2-32 混合认证模板高级配置

页面详细说明如表 2-17 所示。

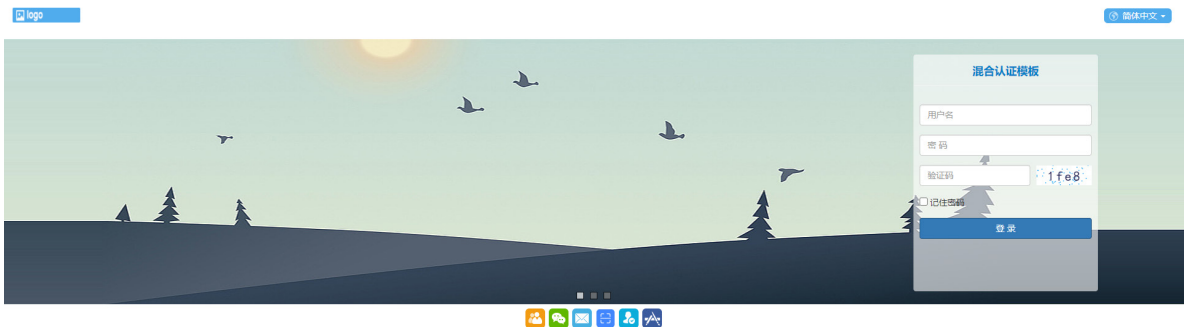
表2-17 混合认证模板高级配置详细说明

项目	说明
发送按钮颜色	短信认证发送短信验证码的按钮颜色。
免认证描述	免认证描述信息。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

点击预览图标查看 PC 终端预览效果，如图 2-33 所示。

图2-33 混合认证模板 PC 终端预览效果



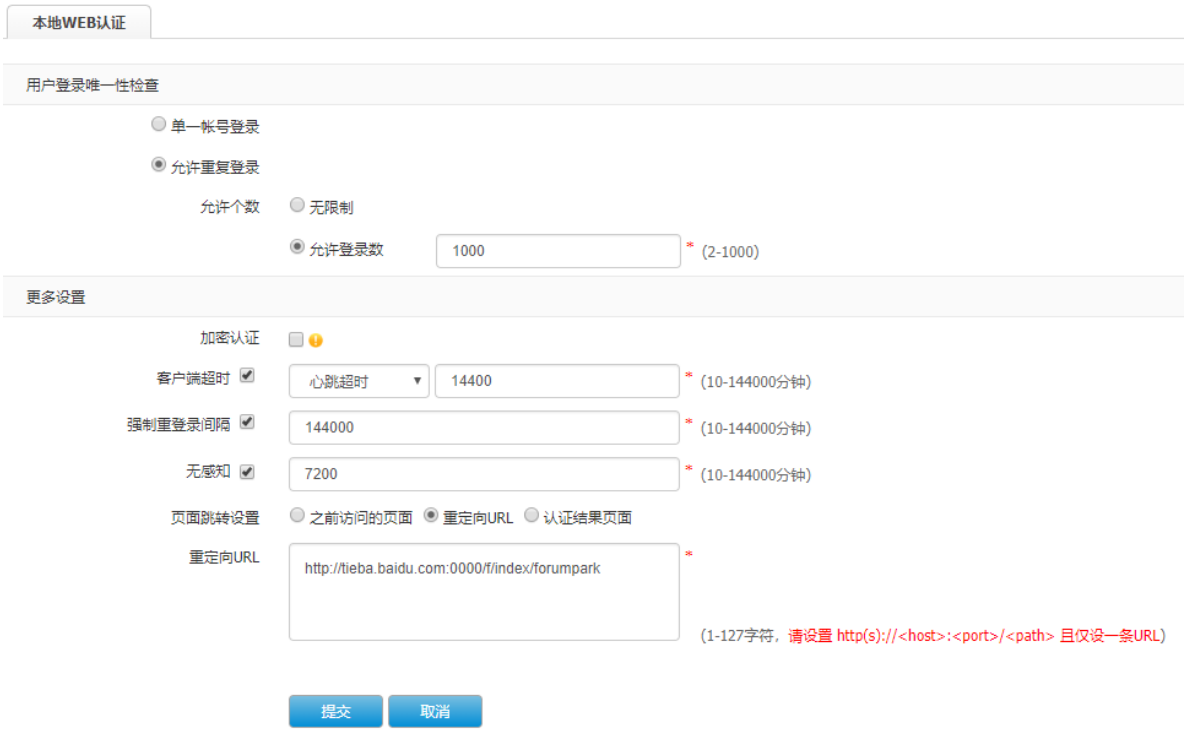
点击预览图标查看移动终端预览效果，如图 2-34 所示

图2-34 混合认证模板移动终端预览效果

2.3.2 本地 WEB 认证配置

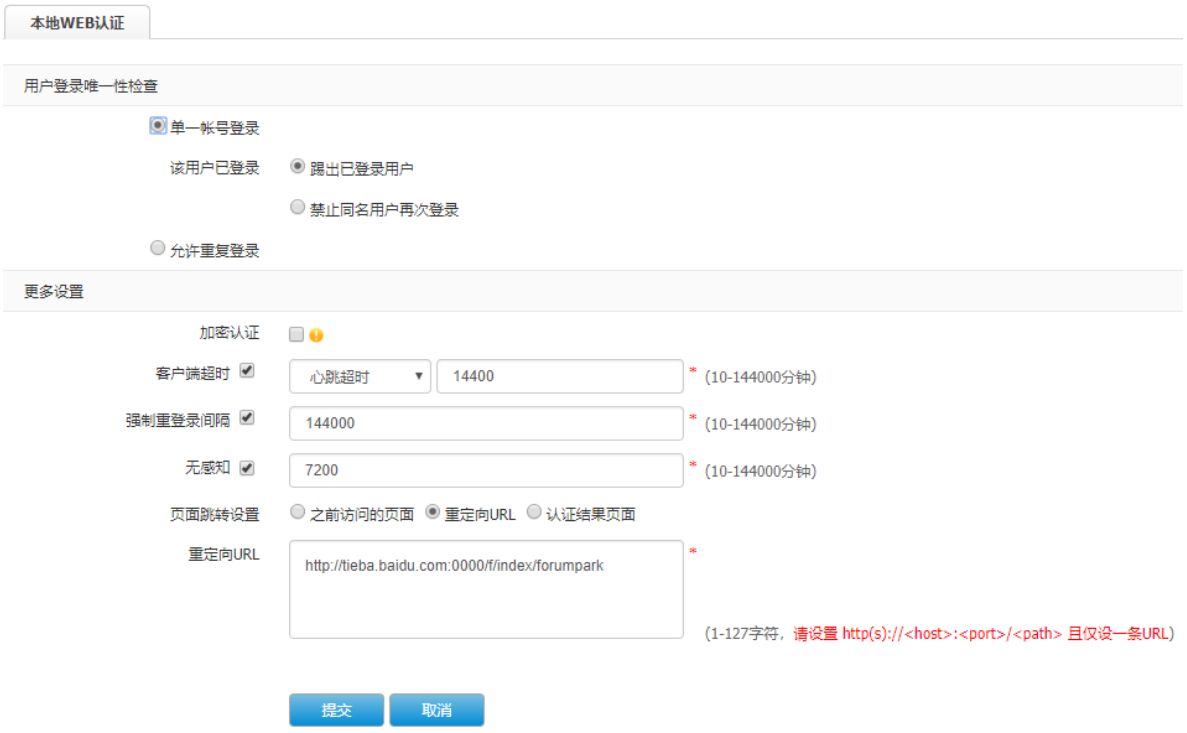
在导航栏中选择“用户管理 > 认证管理 > 认证方式 > 本地 WEB 认证”，进入本地 WEB 认证配置页面，页面显示了当前的本地 WEB 认证配置，如图 2-35 所示。

图2-35 本地 WEB 认证配置页面(允许重复登录)



系统默认选择允许重复登录，如果选择单一账号登录点选框，页面如图 2-36 所示。

图2-36 本地 WEB 认证配置页面(单一账号登录)



页面的详细说明如表 2-18 所示。

表2-18 本地 WEB 认证配置详细说明

项目	说明
用户唯一性检查	用户唯一性检查的配置方式。
单一账户登录	同一时间只允许同一账号登录一次。
踢出已登录用户	如果新用户登录，老的用户将会被踢下线。
禁止同名用户再次登录	如果老用户已经登录，新用户将不能以此用户名登录。
允许重复登录	同一时间允许同一账号登录多次。
允许个数	允许同一账号登录的次数，可以选择无限制，也可以设定2到1000的数值。
加密认证	勾选后，认证过程中对终端与设备之间的认证报文进行加密处理。 如密码存储在LDAP、RADIUS等第三方服务器上，终端与设备之间的认证报文进行加密处理，但设备与服务器之间的交互报文不加密。
客户端超时	配置客户端超时方式和超时时间，超时方式包含：心跳超时、流量超时。 心跳超时：用户认证上线后的页面会定期发心跳报文，如果页面关闭心跳报文会停止发送，如果超过超时时间设备未收到心跳报文会将用户踢下线发送； 流量超时：设备检测用户产生流量，如果超过超时时间都未检测到用户流量会将用户踢下线 ； 不勾选超时时间默认不超时
强制重登录间隔	WEB强制重新认证时间。如果开启无感知，用户被强制重登录踢下线后，会重新匹配无感知上线。
无感知	配置用户无感知认证功能及超时时间，默认值10080分钟。 无感知功能适用于用户下线后再次上线时，MAC地址不变的场景，实现已认证过的终端无感知上线，实现原理如下： 当认证用户上线后会将用户MAC加入无感知列表，如果用户因超时下线，在无感知周期内，用户使用同一终端（MAC地址不变）再次上网产生流量时，会直接匹配无感知列表上线，无需再次认证；若大于超时时间，设备会将该用户MAC从无感知列表中删除，此后用户下次上线时需要重新输入账号密码进行认证。
页面跳转设置	之前访问的页面：WEB认证成功后跳转到用户认证之前访问的页面。 重定向URL：WEB认证成功后将重定向到指定的URL资源页面。 认证结果页面：WEB认证后跳转到认证登录结果页面。

输入完毕后，点击<提交>按钮，应用配置。

说明

无感知认证支持跨三层组网，但需要在设备上开启 SNMP 跨三层 MAC 学习功能，以获取用户的真实 MAC。如果未开启 SNMP 跨三层 MAC 学习功能，会把报文中的三层设备的 MAC 加入到无感知列表，从而导致三层设备下的用户都可以无感知上线了。

2.3.3 微信认证配置

1. 微信认证简介

微信认证支持两种认证方式：

- 通过认证 URL 认证。用户单击公众号指定的超链接（认证 URL），该报文被设备截获，并与设备配置的认证 URL 进行对比，如果匹配则认证成功，并以终端 IP 为用户名上线。
- 通过小程序认证。用户授权小程序完成认证，小程序将获取的 OpenID 和手机号发给设备，设备以此将终端上线。

2. 原理描述

- 通过认证 URL 认证的流程如下：

(1) 用户访问外网触发弹出认证页面，认证页面说明认证的步骤以及商家公众号信息。

(2) 用户单击认证页面上的认证按钮，设备临时放通终端的流量，唤醒微信。

(3) 用户根据认证页面的提示，手动搜索公众号并关注（也可以通过扫码）。然后在公众号中输入关键字（比如：我要上网）或单击菜单。

(4) 公众平台根据之前的配置，对关键字或菜单请求返回认证 URL，并向用户呈现为带超链接的文本信息（比如：点我上网）。

(5) 用户单击该文本信息，微信对认证 URL 发起访问。

(6) 设备劫持该请求，判断是否是微信流量、并与设备配置的认证 URL 进行匹配，并以终端的 IP 为用户名将用户上线，完成微信认证。

- 通过小程序认证的流程如下：

(1) 用户访问外网触发弹出认证页面，认证页面说明认证的步骤以及商家公众号信息。

(2) 用户单击认证页面上的认证按钮，设备临时放通终端的流量，唤醒微信。

(3) 用户根据认证页面的提示，手动搜索公众号并关注（也可以通过扫码）。然后在公众号中输入关键字（比如：我要上网）或单击菜单。

(4) 公众平台根据之前的配置，对关键字或菜单请求推送小程序。

(5) 用户打开小程序，单击授权申请进行 OpenID 和手机号的授权。

(6) 设备创建微信用户对象并上线，完成微信认证。

3. 微信认证配置

在导航栏中选择“用户管理 > 认证管理 > 认证方式 > 微信认证”，进入微信认证配置页面，如下图所示。

图2-37 微信认证配置页面

页面的详细说明如下表所示。

表2-19 微信认证配置页面详细说明

项目	说明
超时时间	微信认证用户超时时间，默认值为15分钟，在时间段内没有流量设备会强制用户下线。
无感知	用户无感知认证功能及超时时间，默认值10080分钟，当认证用户首次认证下线后，在超时时间内再次上网无需认证，可以无感知上线。
用户名	用户名支持IP地址、OpenID、手机号，默认值为IP地址。 使用IP地址，微信公众平台可以配置为关键字回复或者自定义菜单两种方式；使用OpenID、手机号时，微信公众平台需要配置为自定义菜单并关联小程序。
公众号名称	微信公众平台申请的公众号名称，该名称会在认证页面上显示。
应用ID	微信公众平台，开发者中心的开发者ID中的AppId项。
应用密钥	微信公众平台，开发者中心的开发者ID中的AppSecret项。
认证步骤说明	认证步骤说明会在认证页面显示，用以提示用户按步骤完成微信认证。默认认证步骤说明是“请点击认证菜单进行微信认证”，用户可以根据自己公众号的配置进行自定义配置。
认证URL	用户名为ip时为必填项，不可以配置网络中已经存在的url，需要与微信公众平台配置的链接一致；用户名为openid或手机号时为非必填项。

2.3.4 短信认证配置

在导航栏中选择“用户管理 > 认证管理 > 认证方式 > 短信认证”，进入短信认证配置页面，如图 2-38 所示。

图2-38 短信认证配置页面

页面的详细说明如表 2-20 所示。

表2-20 短信认证配置页面详细说明

项目	说明
启用	启用开关，开启后可配置页面其它参数。

项目	说明
超时时间	短信认证用户超时时间，默认值为15分钟。
无感知	用户无感知认证功能及超时时间，默认值10080分钟，当认证用户首次认证下线后，在超时时间内再次上网无需认证，可以无感知上线。
加密认证	勾选为使用加密方式进行认证，防止用户名和密码在传输过程中泄露，如果关闭加密认证会存在安全风险，默认为勾选。
页面跳转设置	之前访问的页面：WEB认证成功后跳转到用户认证之前访问的页面。 重定向URL：WEB认证成功后将重定向到指定的URL资源页面。 认证结果页面：WEB认证后跳转到认证登录结果页面。
厂商	短信网关厂商设置，目前支持凌凯、亿美软通、一信通、佳诺、阿里云、梦网科技、移动云MAS。
短信内容前缀	短信网关发送短信验证码时的短信内容前缀，一般为使用设备的企业或单位名称。
网关地址	网关URL地址，由短信服务商提供。
序列号	短信网关的授权接入序列号，由短信服务商提供。
密码	短信网关的授权接入密码，由短信服务商提供。
短信key	短信服务商提供的短信key，由短信服务商提供，如未设置系统将自动创建。
扩展号段	一个序列号的不同扩展号段，类似“电话分机号”概念，各设备分别设置不同的“扩展号段”，亿美平台根据每一个设备的“拓展号段”通道进行短信验证码发送。此项特性可以避免多个设备使用一个亿美账号发送短信验证码时产生拥堵的情况。
短信内容	定制短信显示内容。长度为1-256个字符，必须包含标签 <identifying-code>，表示验证码。

2.3.5 Portal Server 认证配置

在导航栏中选择“用户管理 > 认证管理 > 认证方式 > Portal Server”，进入 Portal Server 服务器配置页面，如图 2-39 所示。

图2-39 Portal Server 服务器配置页面

页面的详细说明如表 2-21 所示。

表2-21 Port Server 服务器创建页面详细说明

项目	说明
认证服务器	Portal认证使用的radius服务器或radius服务器组名称。
Portal服务器	Portal服务器的IP地址。
快速无感知	用户快速无感知认证功能及超时时间，当认证用户上线后会将用户MAC加入到IMC无感知列表，如果用户因超时下线，在无感知周期内，用户再次上网产生流量时，会根据用户MAC去匹配IMC服务器无感知列表，如果匹配上，则无需再次认证。
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。
认证URL	Portal认证时重定向的URL。

2.3.6 免认证配置

在导航栏中选择“用户管理 > 认证管理 > 认证方式 > 免认证”，进入免认证配置页面，如图 2-40 所示。

图2-40 免认证配置页面

页面的详细说明如表 2-22 所示。

表2-22 免认证配置页面详细说明

项目	说明
超时时间	免认证用户超时时间，默认值为15分钟。
页面跳转设置	之前访问的页面：WEB认证成功后跳转到用户认证之前访问的页面。 重定向URL：WEB认证成功后将重定向到指定的URL资源页面。 认证结果页面：WEB认证成功后跳转到认证登录结果页面。

2.3.7 访客二维码认证

1. 访客二维码认证概述

访客二维码认证主要针对下列两种场景：

- 对于企业访客，联网时，终端弹出认证二维码，由公司内部审核人员（比如前台），扫描二维码，备注访客信息，然后实现访客上网；
- 对于酒店客户，手机可以通过微信认证上网，而笔记本无法进行微信认证，可以选择二维码认证，客户通过已经认证的手机，扫描笔记本二维码完成认证，最终实现笔记本上网。这种方式下，不需要弹出审核页面，直接以审核人身份上网。

2. 访客二维码认证配置

在导航栏中选择“用户管理>认证管理>认证方式 > 访客二维码认证”，进入访客二维码认证页面，页面显示了当前的访客二维码认证配置，如图 2-41 所示。

图2-41 访客二维码认证页面

页面的详细说明如表 2-23 所示。

表2-23 访客二维码认证配置详细说明

项目	说明
超时时间	二维码认证成功用户无流量的情况下超时时间。
二维码超时	二维码认证时二维码超时时间。
无感知	二维码认证成功用户无流量超时下线后，在无感知配置时间内，可以无需认证直接上线。
页面跳转	认证成功后，跳转页面，支持三种： • 之前访问的页面 • 重定向URL • 认证结果页面
审核人	审核人用户配置。
审核方式	支持两种审核方式： • 弹出审核页面，审核备注并授权。 • 不弹审核页面，以审核人身份登录。

输入完毕后，点击<提交>按钮，应用配置。

2.3.8 IC 卡认证

IC 卡认证是在一些上网管控要求严格的场景，用户在使用网络服务时需要使用自己的 IC 卡进行认证等操作后，才允许用户访问网络。

在导航栏中选择“用户管理 > 认证管理 > 认证方式 > IC 卡认证”，进入 IC 卡认证配置界面，如图 2-42 所示。

图2-42 IC 卡配置页面

表2-24 IC 认证配置界面详细说明

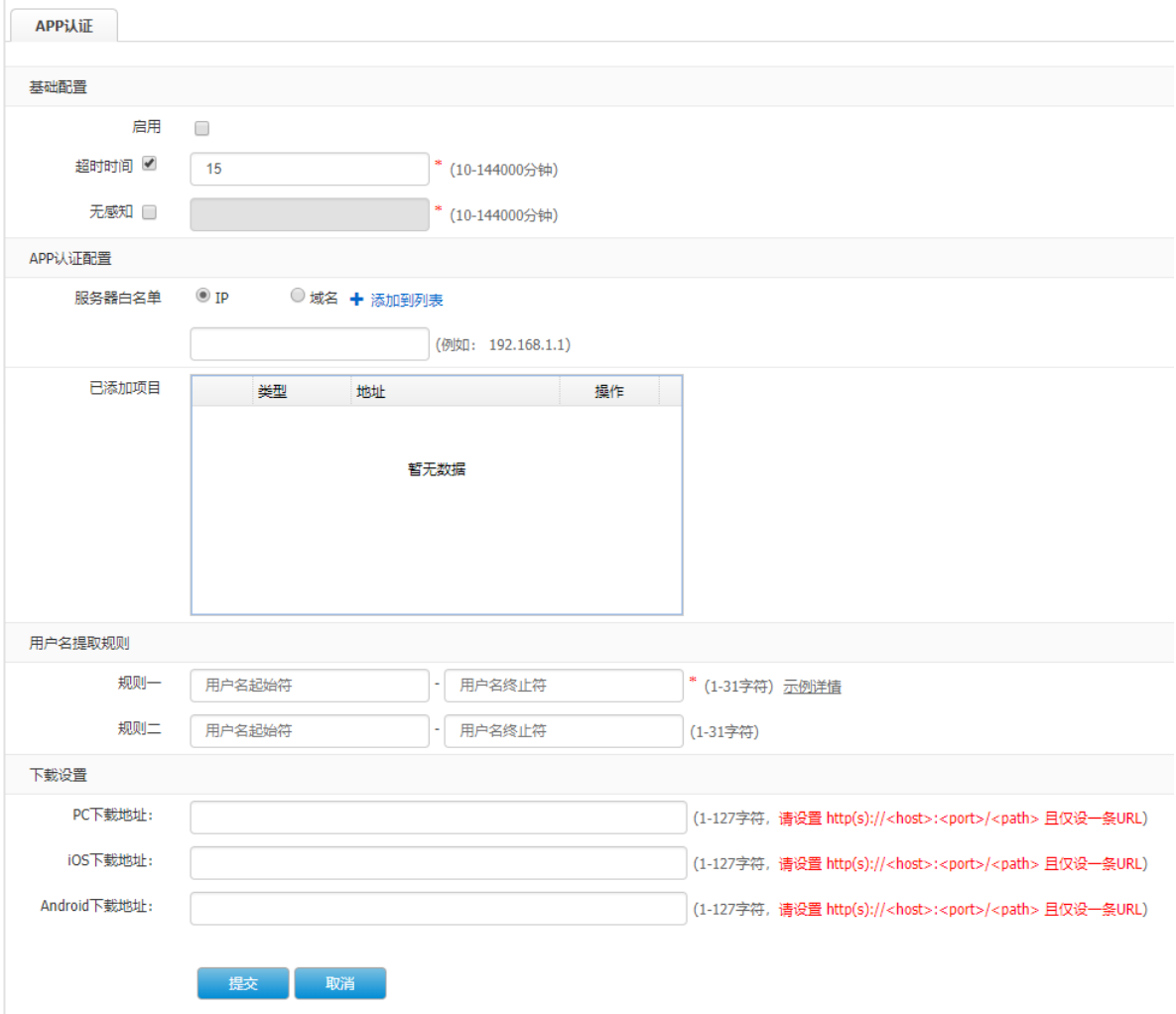
参数	说明
超时时间	IC认证用户超时时间，默认值为15分钟。在时间段内没有流量设备会强制用户下线。

2.3.9 APP 认证

随着手机的普及，手机的使用已是人们生活中不可分割的一部分。手机 APP 已成为时下的主流，不仅为我们的生活带来了极大的便利，还使移动办公成为了可能。因此，在客户场景中使用用户认证功能与 APP 进行联动，从而使认证用户才能使用网络服务。

在导航栏中选择“用户管理 > 认证管理 > 认证方式 > APP 认证”，进入 APP 认证配置界面，如图 2-43 所示。

图2-43 APP 认证配置页面



界面详细说明如表 2-25 所示。

表2-25 APP 认证配置界面详细说明

参数	说明	取值建议
超时时间	APP认证用户超时时间，在时间段内没有流量设备会强制用户下线。	默认值为15分钟，可输入的范围为10-144000分钟。
无感知	用户无感知认证功能及超时时间，当认证用户首次认证下线后，在超时时间内再次上网无需认证，可以无感知上线。	默认值为10分钟，可输入的范围为10-144000分钟。
服务器白名单	添加APP软件下载的服务器地址。	可以输入IP格式或域名格式的地址，单击“添加到列表”。
规则一	添加在app登录url请求中用户名称位置，在规则中填写用户名起始符和用户名终止符，规则一为必填项。	APP账号登录支持GET和POST两种方式。首先使用抓包软件抓整个APP应用登录过程的报文，然后过滤找到包含登录账号的GET报文或POST表单报文，根据报文内容用户名提取规则配置用户名起始

		符。
规则二	添加在app登录url请求中用户名称位置，在规则中填写用户名起始符和用户名终止符，规则二为非必填项。	-
PC下载地址	填写PC端下载APP应用的连接地址。	长度为1-512字符，前缀必须为http或https，且仅可设置一条URL。
IOS下载地址	填写IOS端下载APP应用的连接地址。	长度为1-512字符，前缀必须为http或https，且仅可设置一条URL。
Android下载地址	填写Android端下载APP应用的连接地址。	长度为1-512字符，前缀必须为http或https，且仅可设置一条URL。

2.3.10 POP3 认证

POP3 认证是指用户在使网络服务时，可以在认证页面中输入内网或外网邮箱服务器中的邮箱账号和密码进行认证，从而使认证用户接入使用网络。

在导航栏中选择“用户管理 > 认证管理 > 认证服务器 > 认证服务器”，进入认证服务器界面。将鼠标移至“新建”按钮，在下拉框中选择“POP3 服务器”，进入 POP3 服务器的配置界面，如图 2-9 所示。

在导航栏中选择“用户管理 > 认证管理 > 认证方式 > POP3 认证”，进入 POP3 认证配置界面，如图 2-44 所示。

图2-44 POP3 认证配置页面

表2-26 POP3 认证配置界面详细说明

参数	说明
认证服务器	用户唯一性检查的配置方式。
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。
无感知	用户无感知认证功能及超时时间，默认值10080分钟，当认证用户上线后会将用户MAC加入无感知列表，如果用户因超时下线，在无感知周期内，用户

	再次上网产生流量时，会直接匹配无感知列表上线，无需再次认证。
页面跳转设置	之前访问的页面：认证成功后跳转到认证前访问的页面。 重定向URL：认证成功后将重定向到指定的URL资源页面。 认证结果页面：认证成功后停留在认证结果页面。

POP3 服务器的配置请参见 2.2.3 配置 POP3 服务器。

2.3.11 钉钉认证

1. 简介

用户通过钉钉认证授权的方式进行验证身份后上网。主要应用于企业网络场景，便于企业网络人员通过钉钉应用进行上网行为的管理。

钉钉认证的认证流程如下：

(1) 在设备上配置认证策略。

(2) 对用户 PC 访问外网的流量进行劫持并触发用户认证弹 portal。

(3) 用户获取钉钉授权登录的二维码。

(4) 用户使用手机扫描获取到的二维码，并向钉钉服务器发送确认信息。

(5) 服务器会将确认后的相关信息返回给用户 PC，此时 PC 再通过回调地址将数据发送给设备。

(6) 设备使用用户通过回调地址提供的信息向钉钉服务器获取用户的认证信息。

(7) 用户认证信息获取成功，使用获取到的信息将用户上线。

(8) 用户上线成功后放通后续用户的所有流量。

2. 钉钉认证配置

在导航栏中选择“用户管理>认证管理>认证方式>钉钉认证”，进入钉钉认证配置页面，如下图所示。

图2-45 钉钉认证配置页面

页面的详细说明如表 2-20 所示。

表2-27 钉钉认证配置页面详细说明

项目	说明
启用	是否启用钉钉认证。
超时时间	钉钉认证的超时时间，默认值为15分钟，在时间段内没有流量设备会强制用户下线。
页面跳转设置	设置认证成功之后页面跳转情况。
回调地址	在钉钉服务器用来指定跳转回设备的URL地址，输入格式为：设备管理地址IP+指定端口，目前只支持http。 例如：http://192.168.1.1:8000/ 配置必须和钉钉服务器配置保持一致。

项目	说明
	即在钉钉服务器用来指定跳转回设备的URL地址。
AppID	钉钉服务器配置的AppID。在钉钉开放平台https://open-dev.dingtalk.com设置扫码登录应用授权，钉钉服务器自动生成的个人钉钉的唯一标识
AppSecret	钉钉服务器配置的AppSecret，钉钉服务器自动生成的应用秘钥。
企业ID	钉钉服务器配置的企业ID，从钉钉认证服务器获取的enterpriseid（企业id）唯一标识。
Appkey	钉钉服务器配置的Appkey，自动获取用户组时，需要和钉钉服务器端建立连接，由钉钉服务器端生成的公钥。
自动获取所属组	选择是否自动获取所属组。
路径	开启自动获取所属组时，会将认证用户自动获取并在“数据中心>系统监控>在线用户>属性组>认证用户”中显示；同时可以手动配置认证用户所属路径。

2.3.12 混合认证

混合认证是指认证策略中认证方式为混合认证，混合方式可以选择一种或者多种认证，在用户弹出的认证页面中可以选择其中一种进行认证即可。

在导航栏中选择“用户管理 > 认证管理 > 认证方式 > 混合认证”，进入混合认证配置界面。

图2-46 混合认证配置页面

表2-28 混合认证配置界面详细说明

参数	说明
页面跳转设置	之前访问的页面：认证成功后跳转到认证前访问的页面； 重定向URL：认证成功后将重定向到指定的URL资源页面； 认证结果页面：认证成功后停留在认证结果页面。

在导航栏中选择“用户管理 > 认证管理 > 认证策略”，进入认证策略配置界面，勾选启用，认证方式选择“混合认证”，并勾选一个或多个认证方式。认证方式支持微信认证、本地 WEB 认证、短信认证、访客二维码认证等。

图2-47 混合认证配置页面

认证方式的配置请参考相关认证方式的配置章节。

2.4 第三方用户同步

2.4.1 第三方用户同步接口

在导航栏中选择“用户管理>认证管理>高级选项>第三方用户同步>第三方用户同步接口”，进入第三方用户同步配置页面，如图 2-48 所示。

图2-48 第三方用户同步配置页面

页面的详细说明如表 2-29 所示。

表2-29 第三方用户同步接口配置详细说明

项目	说明
第三方用户同步接口	
服务器1/服务器2	是否启用第三方用户同步接口功能。开启第三方用户同步接口功能后，第三方认证服务器将用户上线下报文发送到设备的UDP9999端口，设备通过上下线报文来识别用户。支持同时配置两个对接服务器。
服务器名称	第三方认证服务器的名称。
服务器地址	第三方认证服务器的IP地址。
密钥	与第三方认证服务器之间对接的密钥，需要与对端保持一致。

输入完毕后，点击<提交>按钮，应用配置。

2.4.2 Radius 用户同步

在导航栏中选择“用户管理>认证管理>高级选项>第三方用户同步>Radius 用户同步”，进入 Radius 用户同步配置页面，如图 2-49 所示。

图2-49 Radius 用户同步配置页面

页面的详细说明如表 2-30 所示。

表2-30 Radius 用户同步配置详细说明

项目	说明
Radius用户同步	
启用	是否启用Radius用户同步，启用该功能后，用户的Radius报文经过设备，即可通过Radius报文来识别用户。
Radius认证端口	Radius服务器上认证报文的接收端口，默认为1812。支持修改成其它使用的端口.
Radius计费端口	Radius服务器上计费报文的接收端口，默认为1813。支持修改成其它使用的端口.
用户组	用户同步的目的用户组。通过Radius报文识别的用户加入到配置的用户中。

配置完毕后，点击<提交>按钮，应用配置。

2.4.3 web 用户同步（http 流量经过设备）

在导航栏中选择“用户管理>认证管理>高级选项>第三方用户同步>web 用户同步”，进入 web 用户同步配置页面，如图 2-50 所示。

图2-50 web 用户同步(http 流量经过设备)配置页面

页面的详细说明如表 2-31 所示。

表2-31 web 用户同步(http 流量经过设备)配置详细说明

项目	说明
web用户同步(http流量经过设备)	
启用	是否启用web用户同步，启用该功能后，用户的http认证报文经过设备，即可通过http认证报文来识别用户。
web服务器	配置web服务器，支持域名、IP地址、IP地址加端口。
类型	支持从URL请求参数、Cookie值、post表单中获取认证用户名。
url请求参数	对应的报文字段中查询配置的用户名关键字，配置用户名获取类型为url请求参数时配置对应url参数名；配置用户名获取类型为Cookie值时配置对应Cookie名；配置用户名获取类型为POST表单时配置对应用户表单名称。
用户组	用户默认属于web用户组，可以修改所属用户组。
启用认证关键字	是否启用认证关键字，启用该功能后，支持校验服务器响应。
认证成功关键字	启用认证成功关键字后，响应报文匹配到配置的认证成功关键字后用户才可上线，否则用户上线失败。
认证失败关键字	启用认证失败关键字后，响应报文匹配到配置的认证失败关键字后用户上线失败，否则用户上线。

输入完毕后，点击<提交>按钮，应用配置。

2.4.4 web 用户同步（http 流量到达设备）

在导航栏中选择“用户管理>认证管理>高级选项>第三方用户同步>web 用户同步”，进入 web 用户同步配置页面，如下图所示。

图2-51 web 用户同步(http 流量到达设备)配置页面

页面的详细说明如表 2-31 所示。

表2-32 web 用户同步(http 流量到达设备)配置详细说明

项目	说明
web用户同步（http流量到达设备）	
启用	是否启用web用户同步，启用该功能后，用户的http认证报文达到设备，即可通过http认证报文来识别用户。
URL	配置url，http请求的资源路径。
服务器端口	配置用于接收第三方认证报文的设备服务端口。
用户组	用户默认属于web用户同步，可以修改所属用户组。
启用上线信息同步	是否启用上线信息同步，启用该功能后，支持匹配到配置上线信息后用户上线。
上线标记	认证上线请求报文匹配到上线标记后用户才可上线，否则用户上线失败。
上线用户名	认证上线请求报文匹配到上线用户名起始及终止符后用户才可上线，否则用户上线失败。
上线用户IP	认证上线请求报文匹配到上线用户ip的起始及终止符后用户才可上线，否则用户上线失败。
上线用户MAC	认证上线请求报文匹配到上线用户mac起始及终止符后用户才可上线，否则用户上线失败。

项目	说明
启用下线信息同步	是否启用下线信息同步，启用该功能后，支持匹配到配置下线信息后用户下线。
下线标记	认证下线请求报文匹配到上线标记后用户才可下线，否则用户下线失败。
下线用户名	认证下线请求报文匹配到下线用户名起始及终止符后用户才可下线，否则用户下线失败。
下线用户IP	认证下线请求报文匹配到下线用户ip的起始及终止符后用户才可下线，否则用户下线失败。
下线用户MAC	认证下线请求报文匹配到下线用户mac起始及终止符后用户才可下线，否则用户下线失败。

输入完毕后，点击<提交>按钮，应用配置。

2.4.5 其它用户同步

在导航栏中选择“用户管理>认证管理>高级选项>第三方用户同步>其它用户同步”，进入其它用户同步配置页面，如图 2-52 所示。

图2-52 其它用户同步配置页面

页面的详细说明如表 2-33 所示。

表2-33 其它用户同步配置详细说明

项目	说明
其它用户同步	
深澜	勾选表示与深澜认证服务器对接。开启此功能后，配置深澜服务器发送相应的报文到设备，即可识别用户。
城市热点	勾选表示与城市热点认证服务器对接。开启此功能后，配置城市热点服务器发送相应的

项目	说明
	报文到设备，即可识别用户。
PPPOE	勾选表示与PPPOE服务器用户同步。通过PPPoE报文识别用户并在本地用户界面创建相应的用户PPPOE账号。
安美	勾选表示与安美认证服务器对接。开启此功能后，配置安美服务器发送相应的报文到设备，即可识别用户。
ddi终端用户	勾选表示与ddi设备对接。开启此功能后，配置ddi设备发送相应的报文到设备，即可关联终端用户使用的终端型号。

输入完毕后，点击<提交>按钮，应用配置。

2.5 全局配置

在导航栏中选择“用户管理>认证管理>高级选项>全局配置”，进入全局配置页面，页面显示了当前的识别配置和认证配置，如图 2-53 所示。

图2-53 全局配置页面

页面的详细说明如表 2-34 所示。

表2-34 全局配置详细说明

项目	说明
识别范围	标示用户识别范围的地址对象或者地址对象组。 用户只有同时在用户识别范围内和相应的认证网段中，使用流量的时候才会触发认证过程。如该用户不在用户识别范围内，则不会触发认证过程，也不会识别为匿名用户；如该用户在用户识别范围内，但不在任何一个认证网段中，则该用户被识别为匿名用户。
识别模式	识别模式分为“启发模式”和“强制模式”两种，默认配置为强制模式，识别范围默认配置均为 private 私网地址段。 “启发模式”指的是，优先将属于识别范围的 IP 地址识别为在线用户，并且根据流量发起方先识别源 IP，再识别目的 IP，如果源 IP 和目的 IP 都不在识别范围中时则将源 IP 识别为在线用户。 “启发模式”使用场景：对用户识别要求不严格的情况下使用启发模式，在线用户中会出现非识别范围内的用户（如：同时出现私网 IP 和公网 IP 的用户），所以统计到的在线用户数量会比较多，在此模式下需要将识别范围修改成内网实际使用的地址网段，否则会导致用户识别不精确。 “强制模式”指的是，只将属于识别范围的 IP 地址识别为在线用户，并且根据流量发起方先识别源 IP，再识别目的 IP，只有源 IP 或目的 IP 地址中的一个属于识别范围时，才会被识别为在线用户；否则此 IP 地址流量不受系统转发流程中用户识别后的所有功能模块限制，如：用户策略、安全策略、应用识别和审计、入侵检测、病毒防护、QOS。 “强制模式”使用场景：对用户识别要求严格的情况下使用强制模式，在线用户中只会存在识别范围内的用户，过滤掉了不属于内网地址段的用户，精简了在线用户列表，只显示用户真正关心的数据，同时提升了设备性能，不在识别范围内的 IP 流量不走用户认证流程，避免了对用户不关心数据的处理，在此模式下务必将识别范围修改成内网实际使用的地址网段，避免因识别范围配置错误导致的用户关心的 IP 地址流量不受用户策略控制的情况出现。
启用第三方认证	是否启用第三方认证。
认证方式	第三方认证服务器是Radius服务器或者Ldap服务器。
RADIUS	选择已配置的Radius服务器或服务器组。
Ldap	选择已配置的Ldap服务器或服务器组。
https弹portal	勾选后，用户在访问HTTPS网站时也可以弹出认证页面。
用户MAC感知	开启用户MAC感知后，如检测到用户的MAC地址发生变化，则强制用户重新认证。（开启跨三层MAC地址学习功能时会发生用户MAC地址变更的情况。）
伪Portal抑制	对于Portal重定向支持HTTP302方式和Html-refresh方式，选择HTTP302方式时对所有请求都响应，伪Portal抑制不生效；选择Html-refresh方式时，只响应浏览器的请求，伪Portal抑制生效。
用户认证验证码	只对本地认证、免认证、pop3认证、混合认证（本地认证、免认证）生效。
绑定范围与密码同时校验	开启后会同时校验用户绑定的IP/MAC和用户名密码

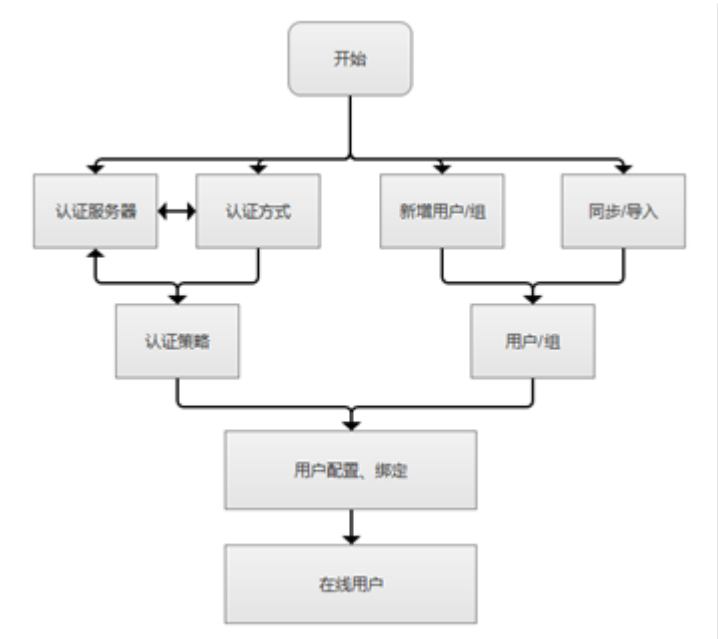
输入完毕后，点击<提交>按钮，应用配置。

2.6 用户认证策略

2.6.1 用户认证策略概述

认证策略录入配置主要针对第三方用户，目的是将存在于第三方的用户加入设备，便于做策略限制等。

图2-54 用户认证策略流程图



2.6.2 认证策略配置

在导航栏中选择“用户管理 > 认证管理 > 认证策略”，单击<新建>按钮，进入认证策略的配置界面，如图 2-55 所示。

图2-55 认证策略配置界面

认证策略参数详细说明，如表 2-35 所示

表2-35 认证策略配置参数详细说明

标题	说明
启用	认证策略启用或禁用，认证策略只有启用才能生效。
名称	认证策略的名称。
描述	认证策略描述信息填写。
源接口	认证策略源接口。
源地址	认证策略源地址对象或地址组，可直接新建地址对象。
目的接口	认证策略目的接口。
目的地址	认证策略目的地址对象或地址组，可直接新建地址对象。
认证方式	认证策略认证方式可选WEB认证、Portal Server认证、短信认证、免认证、微信认证、混合认证、单点登录、二维码认证、IC卡认证、APP认证、POP3认证、钉钉认证。

时间	认证策略时间对象，时间对象有效期内策略生效，时间对象无效的时候认证策略为禁用状态。
用户组	默认不选择用户组，第三方用户认证成功后不录入用户；选择用户组后，第三方用户认证成功后录入指定的用户组。 该功能主要针对于第三方认证的用户，目的将存储在第三方服务器的用户导入设备。如果需要对第三方认证的用户进行策略限制等，建议选择录入指定的用户组。
用户有效时间	用户有效期指的是第三方用户录入方式： • 永久录入：第三方用户认证成功后录入指定组，永久有效。 • 有效期至：第三方用户认证成功后录入指定组，设备运行时间到配置的时间当天 23:59 后，录入的用户状态变为不启用，认证策略也变为不启用。 • 临时录入：第三方用户认证成功后录入指定组，用户注销下线后，录入的用户组里用户自动删除。

2.7 配置举例

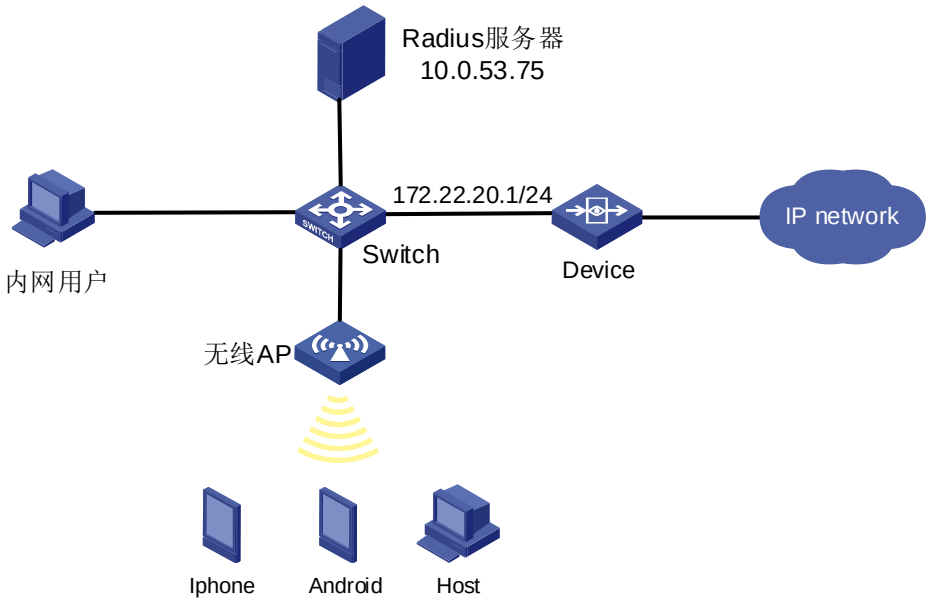
2.7.1 用户认证策略配置举例

1. 组网需求

如图 2-56 所示，某公司内网搭建有第三方 Radius 服务器，用户名全部存放在 radius 服务器上，要求内网用户使用 radius 服务器上的用户进行认证，认证成功后用户录入设备进行其它策略控制。具体要求如下：

- 内网用户进行 Web 认证上网，用户名和密码存储在 Radius 服务器上，认证成功后用户永久录入设备。
- 其它移动终端连接 wifi 后使用微信认证上网，认证策略用户录入为临时录入，用户下线后删除录入用户。

图2-56 用户认证组网图



2. 配置步骤

(1) 添加 Radius 服务器

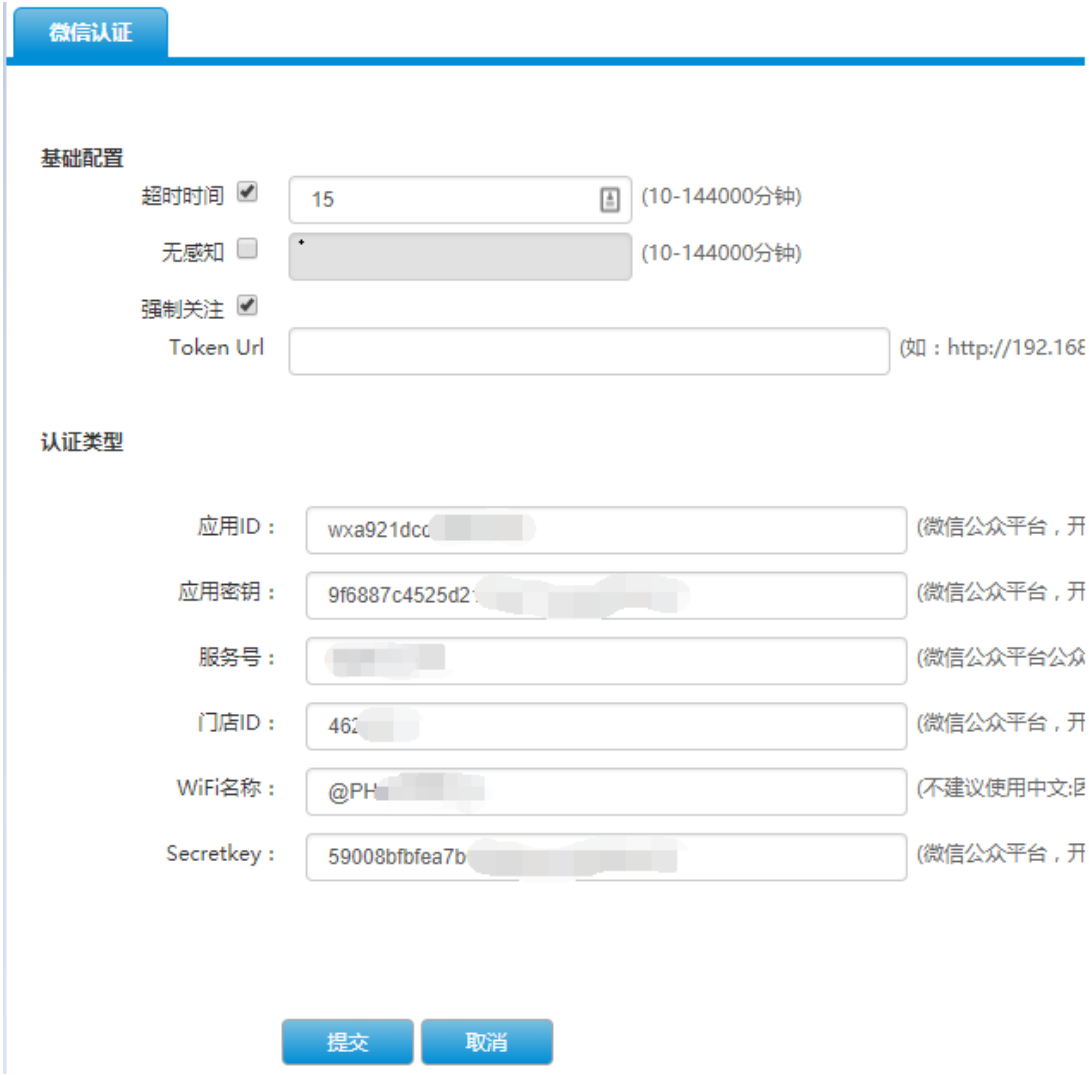
通过菜单“用户管理>认证管理>认证服务器>认证服务器”，选择“新建>Radius 服务器”，配置“服务器地址”为 10.0.53.85，“服务器密码”和“端口”需要和 Radius 服务器保持一致，点击<提交>，如图 2-57 所示。

图2-57 添加 Radius 服务器

(2) 配置微信认证

通过菜单进入“用户管理>认证管理>认证方式>微信认证”，配置微信认证相关参数后，点击<提交>，如图 2-58 所示。

图2-58 微信认证配置页面



(3) 配置地址对象

通过菜单“策略配置>对象管理 > 地址对象”，点击<新建>地址对象，配置内网用户和无线 wifi 地址对象。如图 2-59、图 2-60 所示。

图2-59 添加内网用户地址对象

图2-60 添加用户认证地址对象

(4) 配置用户组对象

通过菜单“用户管理>用户组织结构”，单击<新建>用户组，配置 radius 用户组和无线 wifi 用户组，如图 2-61、图 2-62 所示。

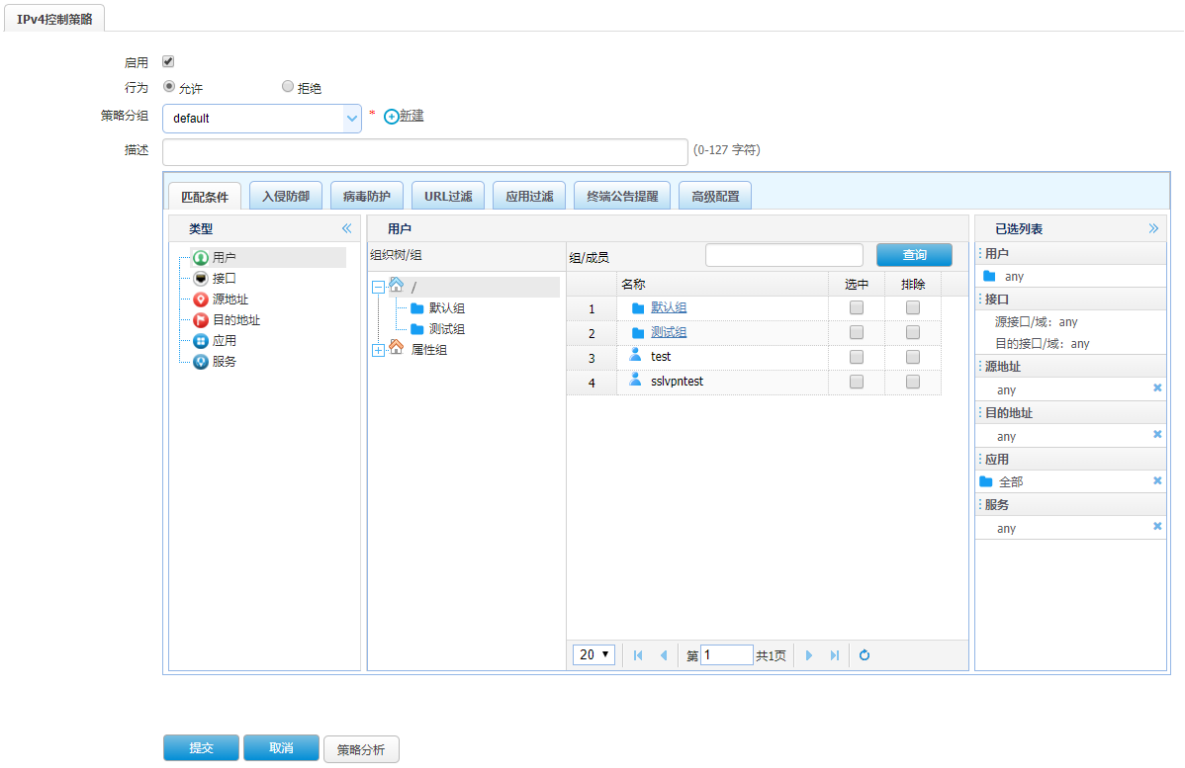
图2-61 配置 Radius 用户组

图2-62 配置无线用户组

(5) 配置 IPv4 控制策略

通过菜单“策略配置>IPv4 控制策略”，点击<新建>IPv4 控制策略，使用默认配置，如图 2-63 所示。

图2-63 IPV4 控制策略配置



(6) 全局配置启用第三方认证选择 radius 服务器

在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证选择 radius 服务器，如图 2-64 所示。

图2-64 全局模式启用第三方 radius 配置效果图

(7) 配置用户策略

a. 配置内网用户认证策略，用户永久录入。

通过菜单进入“用户管理>认证管理>认证策略”，点击<新建>，源地址配置为“内网用户地址对象”，相关行为配置为“本地 Web 认证”，用户录入选择创建的“Radius-group”，有效期为永久录入，点击<提交>。如图 2-65 所示。

图2-65 配置内网用户认证用户策略

(8) 配置无线 wifi 用户认证策略，用户临时录入。

通过菜单进入“用户管理>认证管理>认证策略”，点击<新建>，源地址配置为“无线 wifi 地址对象”，相关行为配置为“微信认证”，用户录入选择创建的“无线 wifi”，用户有效期为临时录入，点击<提交>。如图 2-66 所示。

图2-66 配置无线 wifi 用户认证后临时录入用户策略

3. 验证结果

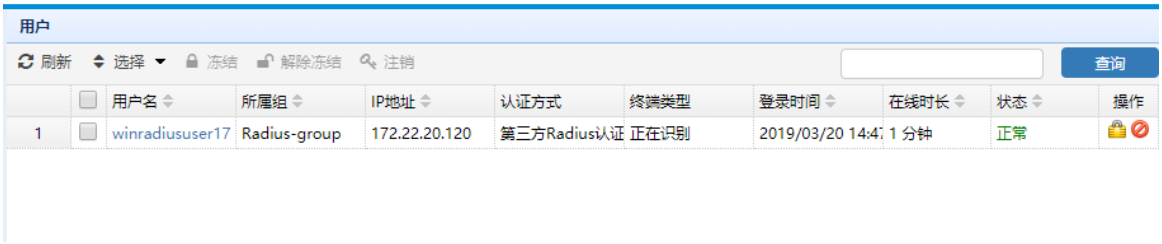
(1) 内网用户用户录入验证

如图 2-67 所示，内网终端进行 HTTP 访问，弹出如下本地 Web 认证页面，使用 radius 服务器上用户名、密码进行认证。

图2-67 内网用户使用第三方 radius 用户认证成功

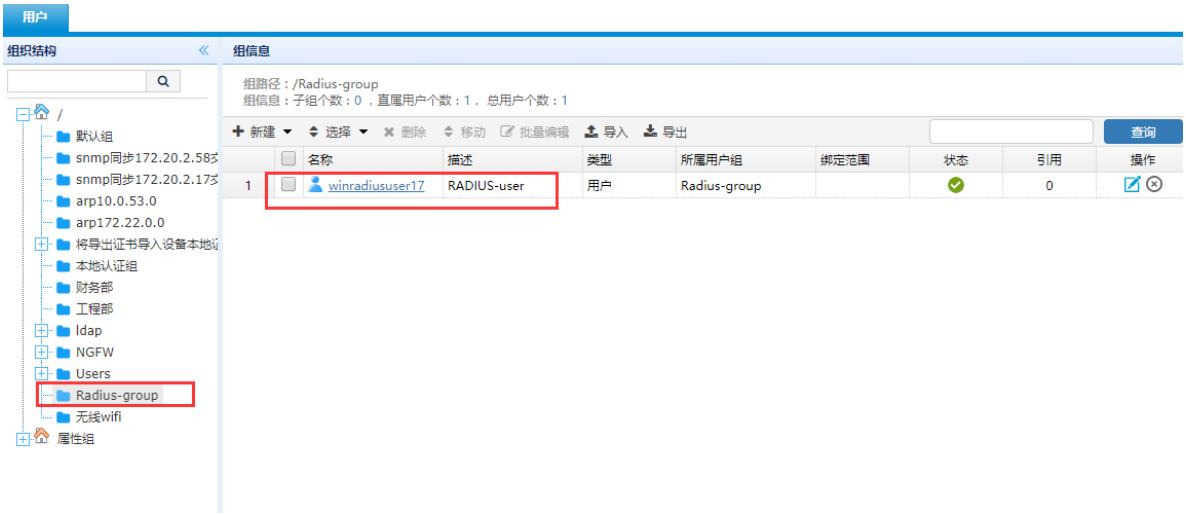
如图 2-68 所示，设备在线用户显示第三方 radius 用户认证。

图2-68 Radius 联动用户 Web 认证成功



通过菜单“用户管理>用户组织结构”，查看 Radius-group 用户组下，winradiususer17 用户已录入，如图 2-69 所示。

图2-69 Radius 用户组下录入用户



如图 2-70 所示，编辑用户查看用户永不过期。

图2-70 radius 录入用户显示为永不过期

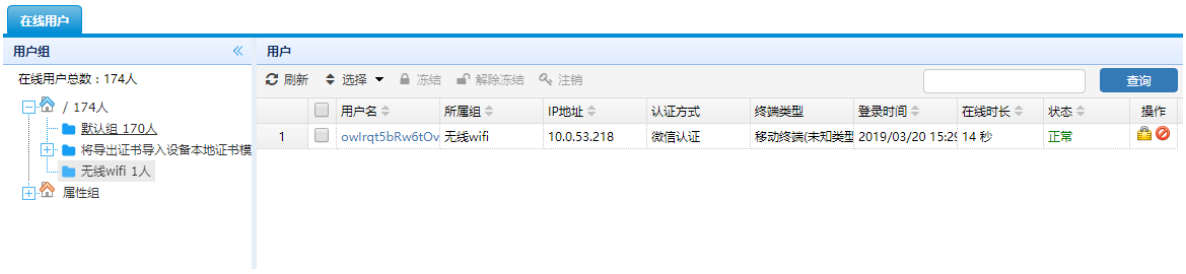
(2) 移动终端用户使用微信认证，用户为临时录入

如图 2-71 所示，移动终端连接 wifi 后浏览器弹出微信认证页面，点击一键打开微信连接进行认证。

图2-71 移动终端连接 wifi 后弹出微信认证页面

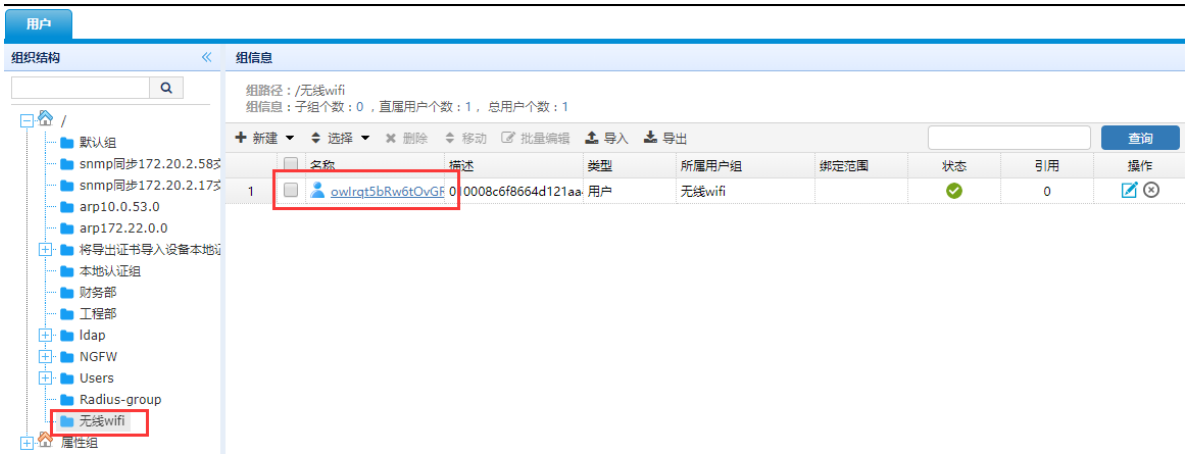
如图 2-72 所示，设备在线用户显示微信认证。

图2-72 微信认证成功



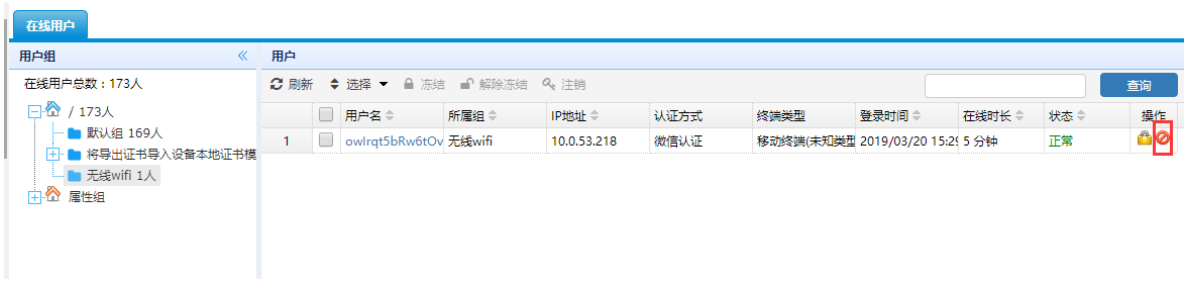
通过菜单“用户管理>用户组织结构”，查看无线 wifi 用户组下，微信用户已录入，如图 2-73 所示。

图2-73 无线 wifi 用户组下录入微信用户



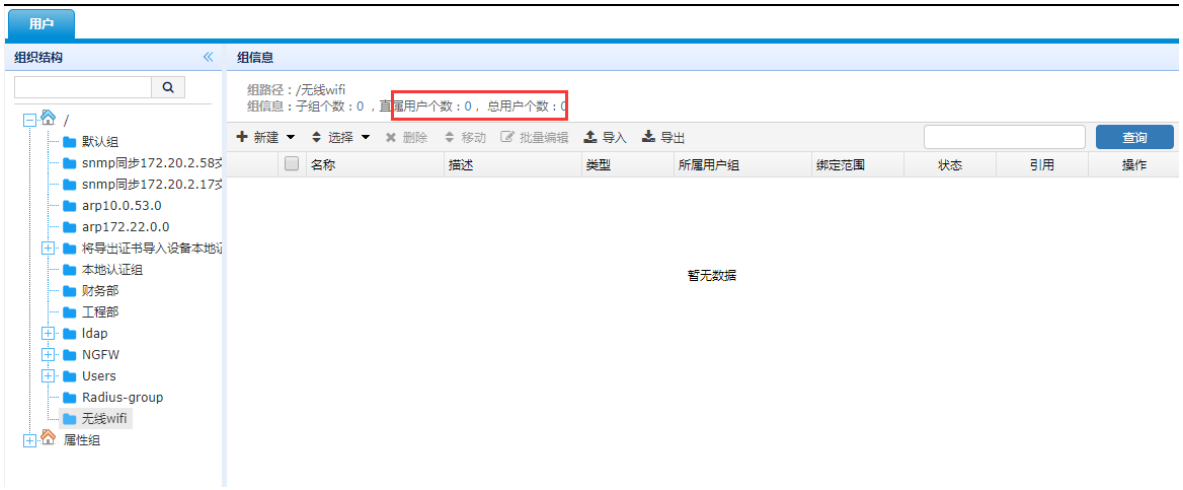
如图 2-74 所示，在线用户处踢出微信认证用户。

图2-74 在线用户踢出微信认证用户



通过菜单“用户管理>用户组织结构”，查看无线 wifi 用户组下，微信用户已删除，如图 2-75 所示。

图2-75 无线 wifi 用户组下录入的微信用户已删除

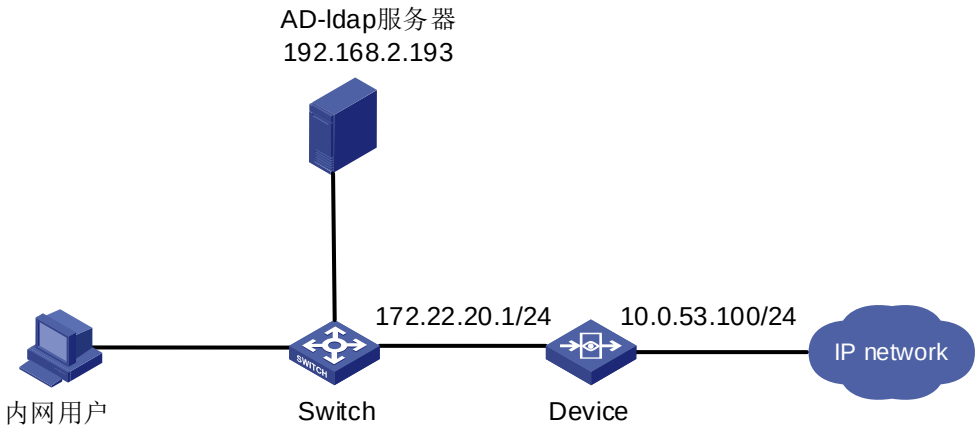


2.7.2 LDAP 使用标识名 CN 认证典型配置举例

1. 组网需求

如图 2-76 所示，在公司你搭建有 LDAP 服务器，LDAP 服务器上用户是以标识名的方式进行创建的，要求内网用户使用 AD-ldap 服务器同步下来的用户进行认证后上网。

图2-76 LDAP 认证拓扑图



2. 配置步骤

(1) 新建 LDAP 服务器，通用名称标识为 cn，并同步。

在导航栏中选择“用户管理>认证管理>认证服务器”，进入认证服务器的配置界面，选择“新建>LDAP 服务器”，配置 LDAP 服务器，如图 2-77 所示。

图2-77 标识为 CN 的 LDAP 服务器配置

配置完成后如图 2-78 所示。

图2-78 LDAP 服务器配置效果图

(2) 新建 LDAP 同步

在导航栏中选择“用户管理>用户同步”，选择“新建>LDAP 同步”，配置 LDAP 同步，如图 2-79 所示。

图2-79 LDAP 同步

(3) 全局模式启用第三方 ldap 配置

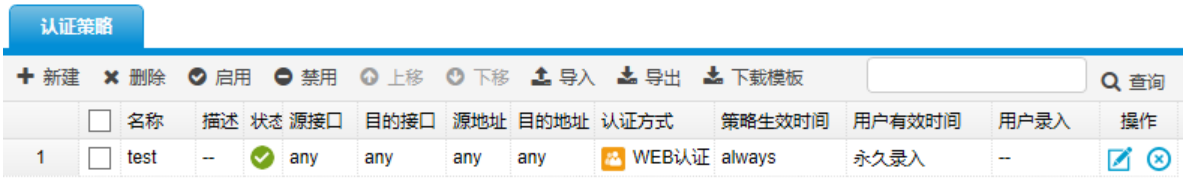
在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证选择 Ldap 服务器，如图 2-80 所示。

图2-80 启用第三方 ldap 配置界面

(4) 新建用户认证策略

在导航栏中选择“用户管理>认证管理>认证策略”，进入用户认证策略的配置页面，单击<新建>按钮，配置认证策略，如图 2-81 所示。

图2-81 用户认证策略配置效果图



3. 验证效果

图2-82 PC 访问网页弹出本地认证界面后，使用同步下来的 LDAP 用户进行认证

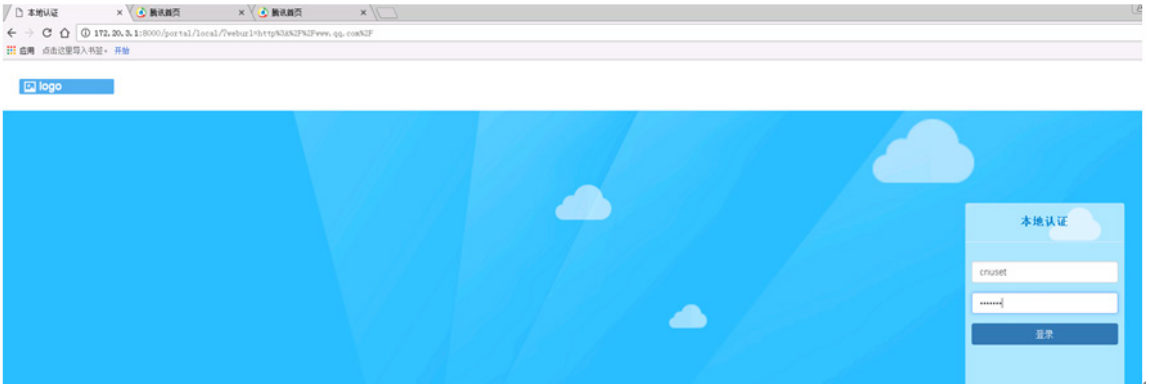
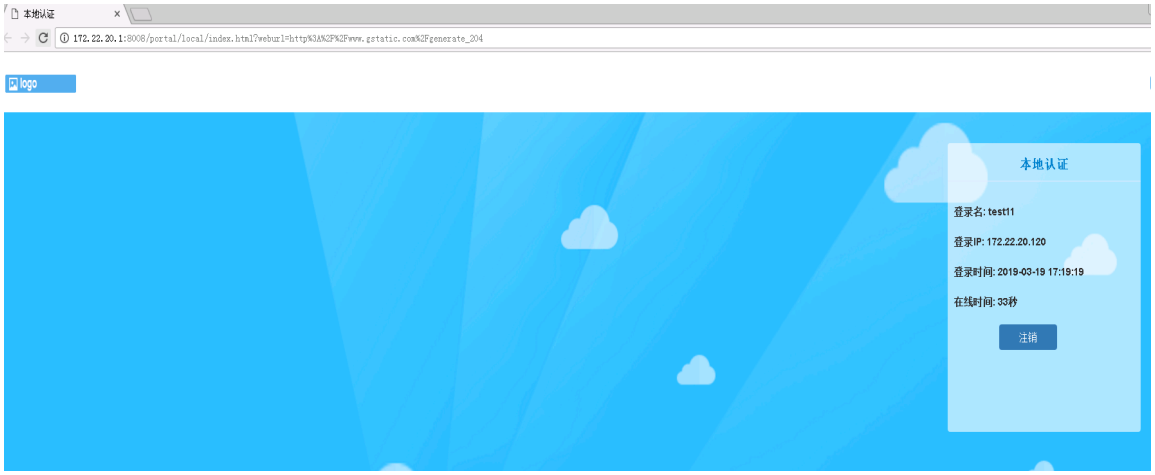


图2-83 认证成功效果图

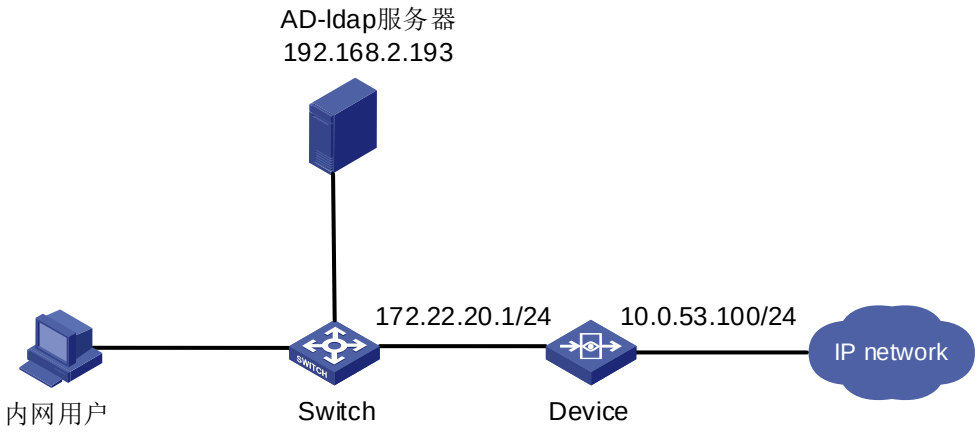


2.7.3 LDAP 使用标识名 sAMAccountName 认证典型配置案例

1. 组网需求

如图 2-84 所示，在公司内网搭建有 LDAP 服务器上用户是以用户登录名的方式进行创建的，要求内网用户使用 AD—ldap 服务器同步下来的用户进行认证上网。

图2-84 LDAP 认证拓扑图



2. 配置步骤

(1) 新建 LDAP 服务器，通用名称标识为 sAMAccountName，并同步。

在导航栏中选择“用户管理>认证管理>认证服务器”，选择“新建 LDAP 服务器”，如图 2-85 所示。

图2-85 标识名为 sAMAccountName 的 LDAP 服务器配置

配置完成后如图 2-86 所示。

图2-86 LDAP 服务器配置效果图

(2) 新建 LDAP 同步

在导航栏中选择“用户管理>用户同步”，选择“新建> LDAP 同步”，配置 LDAP 同步，如图 2-87 所示。

图2-87 LDAP 同步

(3) 全局模式启用第三方 ldap 配置

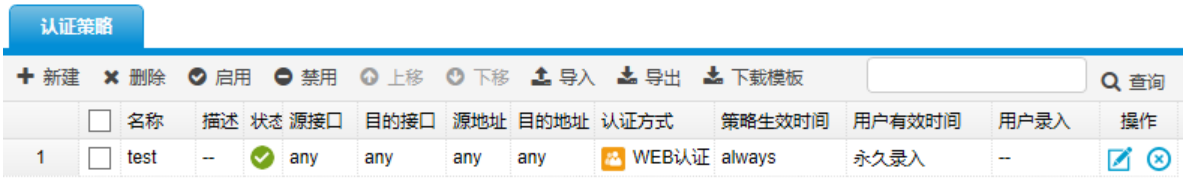
在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证选择 Ldap 服务器，如图 2-88 所示。

图2-88 启用第三方 ldap 配置界面

(4) 新建用户认证策略

在导航栏中选择“用户管理>认证管理>认证策略”，进入用户认证策略的配置页面，单击<新建>按钮，配置认证策略，如图 2-89 所示。

图2-89 用户认证策略配置效果图



3. 验证配置效果

图2-90 PC 访问网页弹出本地认证界面后，使用同步下来的 LDAP 用户进行认证

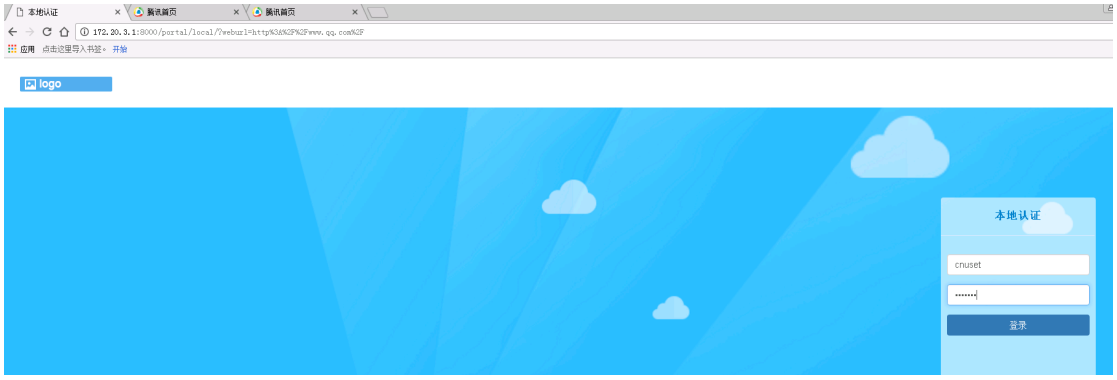
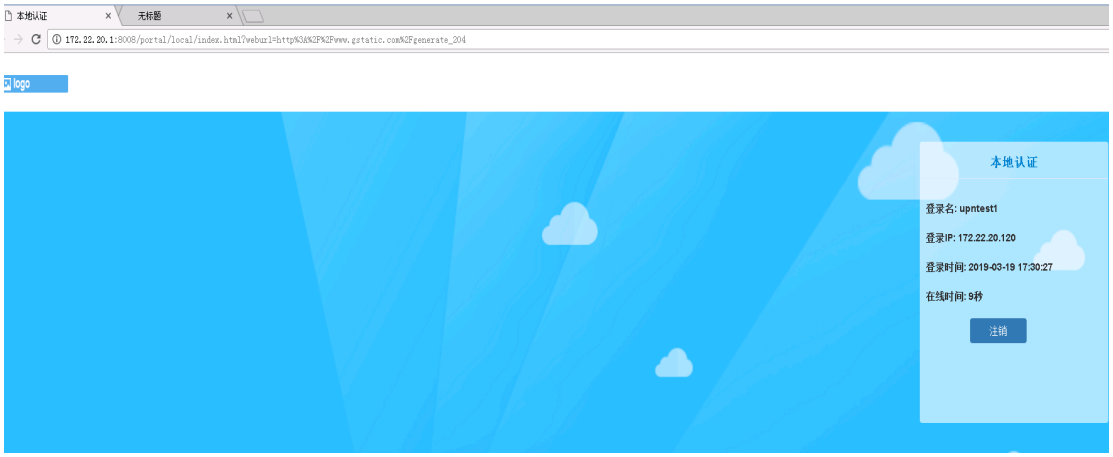


图2-91 认证成功效果图

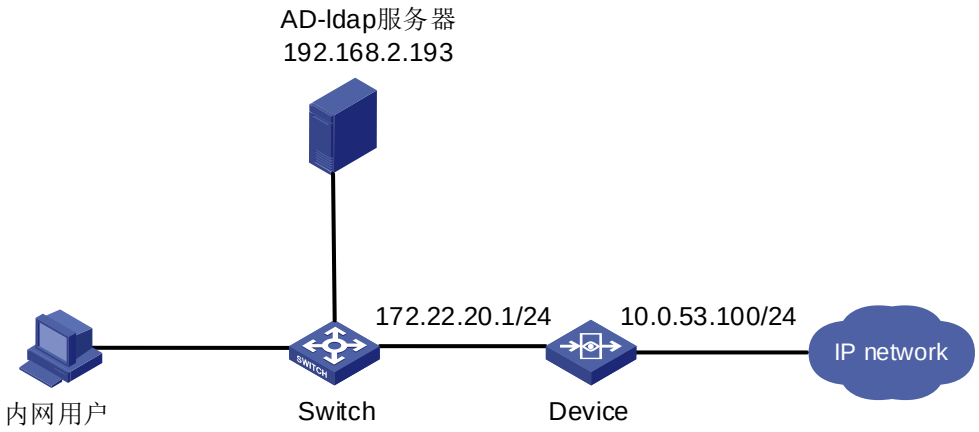


2.7.4 LDAP 控制认证用户名是否区分大小写配置举例

1. 组网需求

如图 2-92 所示，在公司内网搭建有 LDAP 服务器上用户是以用户登录名的方式进行创建的，要求内网用户使用 AD—ldap 服务器同步下来的用户进行认证上网。

图2-92 LDAP 认证拓扑图



2. 配置步骤

(1) 新建 LDAP 服务器，通用名称标识为 sAMAccountName，并同步。

在导航栏中选择“用户管理>认证管理>认证服务器”，单击<新建>按钮，配置 LDAP 服务器，如图2-93 所示。

图2-93 标识名为 sAMAccountName 的 LDAP 服务器配置

配置完成后如图 2-94 所示。

图2-94 LDAP 服务器配置效果图

(2) 新建 LDAP 同步

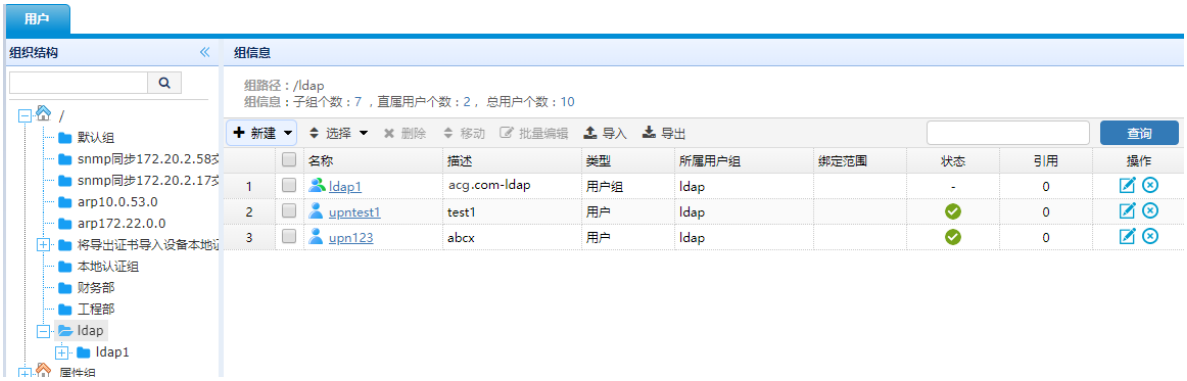
在导航栏中选择“用户管理>用户同步”，选择“新建> LDAP 同步”，配置 LDAP 同步，如图 2-95 所示。

图2-95 LDAP 同步

(3) 查看 LDAP 同步用户

在导航栏中选择“用户管理>用户组织结构”，查看 LDAP 同步用户,如图 2-96 所示。

图2-96 LDAP 同步的用户



(4) 全局模式启用第三方 ldap 配置

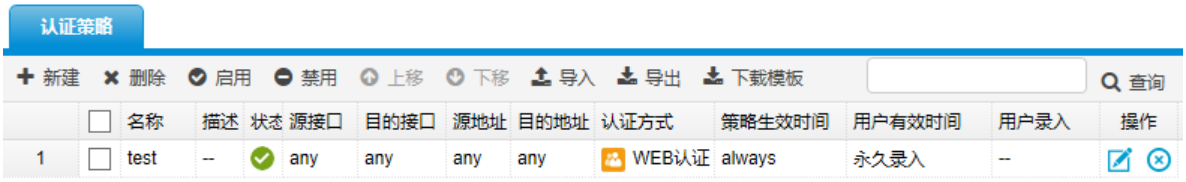
在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证选择 Ldap 服务器，，如图 2-97 所示。

图2-97 启用第三方 ldap 配置界面

(5) 新建用户认证策略

在导航栏中选择“用户管理>认证管理>认证策略”，进入用户认证策略的配置页面，单击<新建>按钮，配置认证策略，如图 2-98 所示。

图2-98 用户认证策略配置效果图



(6) 启用 LDAP 认证用户名不区分大小写，如图 2-99 所示。

图2-99 LDAP 认证用户名不区分大小写配置图

```
(config)# ldap-auth easy-name-match
disable  Disable
enable   Enable
(config)# ldap-auth easy-name-match enable
```

说明

默认情况下设备认证过程中用户名称不区分大小写，而 LDAP 服务器在检验用户名时不区分大小写，如在 LDAP 服务器上配置用户名为 aaa，用户在认证时输入 AAA，也可以认证通过，但在设备侧上线时记录的用户名是 AAA，由于设备从 LDAP 服务器同步下来的用户名是 aaa，其它策略在调用 aaa 做控制后，由于上线时的用户为 AAA，导致策略无法匹配上，为了解决这一问题，设备侧开启认证用户名称区分大小写，即使用户输入了 AAA，上线时也会显示为 aaa，与本地存的用户名一模一样，保证了后续用户对象正常匹配。

3. 验证配置效果

PC 访问网页弹出本地认证页面，后使用同步下来的 LDAP 用户进行认证。（原同步下来的用户为 upntest1，启用 ldap 认证用户名区分大小写后，认证用户名输入 UPNtest1 进行认证）

(1) 关闭 LDAP 认证用户区分大小写

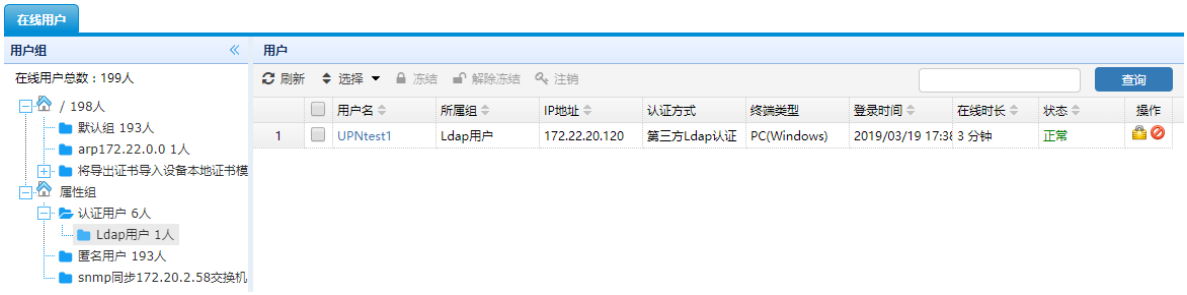
```
WD-D(config)# display ldap-auth easy-name-match switch
ldap-auth easy-name-match disable
```

关闭 ldap 认证用户名区分大小写，认证页面显示如图 2-100 所示。

图2-100 登录页面

关闭 ldap 认证用户名区分大小写，设备在线用户显示如图 2-101 所示。

图2-101 在线用户页面



(2) 开启 LDAP 认证用户区分大小写

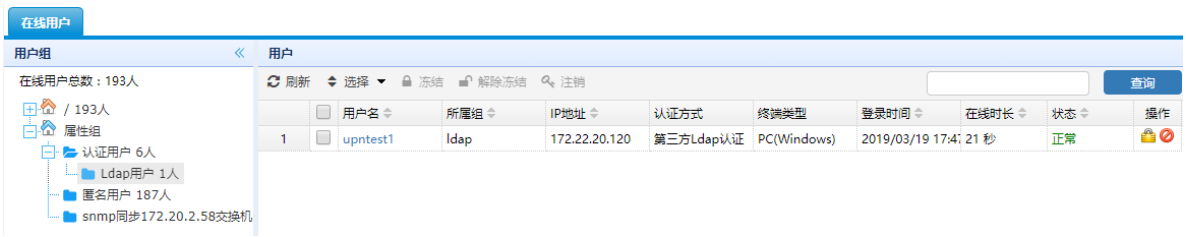
```
[H3C]ldap-auth easy-name-match enable
[H3C]display ldap-auth easy-name-match switch
ldap-auth easy-name-match enable
```

开启 ldap 认证用户名区分大小写，认证页面显示如图 2-102 所示。

图2-102 登录页面

开启 ldap 认证用户名区分大小，设备在线用户显示如图 2-103 所示。

图2-103 在线用户页面

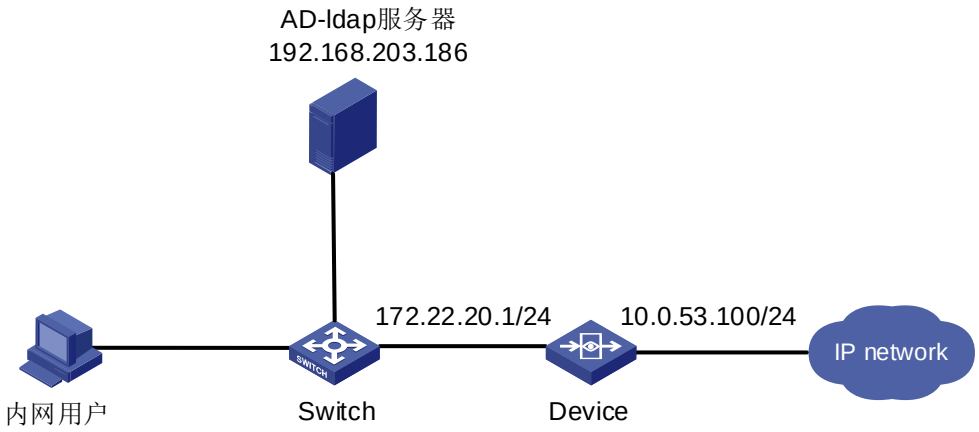


2.7.5 LDAP 使用同步安全组认证配置举例

1. 组网需求

如图 2-104 所示，在公司内网搭建有 LDAP 服务器上用户是以用户登录名的方式进行创建的，要求内网用户使用 AD—ldap 服务器同步下来的用户进行认证上网。

图2-104 LDAP 认证拓扑图



2. 配置步骤

(1) 新建 LDAP 服务器，通用名称标识为 cn。

在导航栏中选择“用户管理>认证管理>认证服务器”，选择“新建>LDAP 服务器”，配置 LDAP 服务器，如图 2-105 所示。

图2-105 标识名为 cn 的 LDAP 服务器配置

(2)　新建 LDAP 同步，同步类型为按安全组同步。

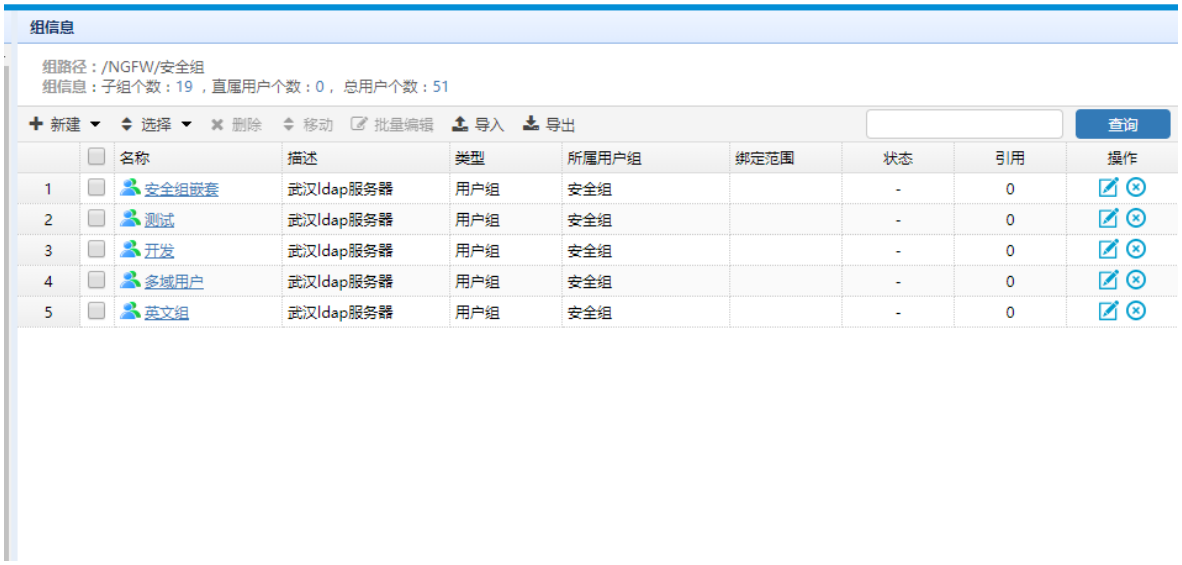
在导航栏中选择“用户管理>用户同步”，选择“新建> LDAP 同步”，配置 LDAP 同步，如图 2-106 所示。

图2-106 LDAP 同步

(3)　查看 LDAP 同步用户

在导航栏中选择“用户管理>用户组织结构”，查看 LDAP 同步用户,如图 2-107 所示。

图2-107 LDAP 同步的用户



(4) 全局模式启用第三方 ldap 配置

在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证选择 Ldap 服务器，如图 2-108 所示。

图2-108 全局模式配置效果图

(5) 新建用户认证策略

在导航栏中选择“用户管理>认证管理>认证策略”，进入用户认证策略的配置页面，单击<新建>按钮，配置认证策略，如图 2-109 所示。

图2-109 用户认证策略配置效果图

3. 验证配置效果

如图 2-110 所示，PC 访问 www.qq.com，弹出本地认证界面。输入 LDAP 同步下来的安全组用户的用户名和密码进行认证。

图2-110 PC 访问网页弹出本地认证页面，后使用同步下来的 LDAP 安全组用户进行认证。

如图 2-111 所示，安全组用户的 LDAP 认证效果图。

图2-111 认证成功效果图

目 录

1 用户同步 ····· 1-1
1.1 概述 ····· 1-1
1.2 原理描述 ····· 1-1
1.2.1 基本原理 ····· 1-1
1.2.2 用户同步流程 ····· 1-2
1.3 配置用户同步 ····· 1-2
1.3.1 用户同步任务查看 ····· 1-2
1.3.2 配置 LDAP 同步 ····· 1-3
1.3.3 配置 SNMP 同步 ····· 1-5
1.3.4 配置 ARP 扫描 ····· 1-6
1.4 用户同步配置举例 ····· 1-7
1.4.1 组网需求 ····· 1-7
1.4.2 配置步骤 ····· 1-8
1.4.3 验证配置 ····· 1-15

1 用户同步

1.1 概述

为了实现用户管理在其使用场景上的易用性，对用户管理相关功能进行优化。用户同步包括 LDAP 同步、SNMP 同步和 ARP 扫描，其中 LDAP 同步需要先配置 LDAP 服务器后，在 LDAP 同步里调用 LDAP 服务器进行同步，LDAP 服务器的配置可参考“用户和用户认证”章节的相关内容。

同步成功录入设备的用户支持在线用户识别、策略调用、QOS 控制、策略路由等模块的引用控制。

1.2 原理描述

1.2.1 基本原理

- LDAP 同步：通过 LDAP 协议报文将 LDAP 服务器上的用户同步到本地，然后可以按照实际需求分别对同步下来的用户组和用户进行相关功能的引用控制，比如：审计策略、控制策略、流控策略、限额策略等，LDAP 同步分为两种同步类型，分别为按 OU(组织单位)同步和按安全组同步，配置为按 OU 同步时即按照 OU 区分所属用户组，按照 LDAP 服务器上 OU 的配置来进行同步，即每个 OU 同步下来后为一个用户组，此 OU 下包含的 OU 和用户也分别对应到此用户组下的用户组和用户，同理配置为按安全组同步时按照安全组区分所属用户组，即每个安全组同步下来后为一个用户组，此安全组下包含的安全组和用户也分别对应到此用户组下的用户组和用户，配置按照 OU 同步时，安全组就不会同步下来作为用户组了，同理如果配置为安全组，那此 BASE DN 下的 OU 也就不会被同步下来作为用户组了；可以开启自动同步，开启自动同步后需配置起始时间和间隔时间，起始时间表示在每天的这个时间点进行同步，间隔时间表示本次执行同步后每经过配置的间隔时间后再执行同步。
- SNMP 同步：通过 SNMP 协议报文获取三层交换机上的 ARP 表，从而得到了内网 PC 真实的 IP 和 MAC 地址对应关系，同步下来的 IP 地址和 MAC 地址的对应关系可以录入到用户组也可以进行 IP-MAC 绑定。录入到用户组支持手工录入和自动录入，录入的用户以 IP 地址作为用户名，绑定其 IP 及 MAC 地址，即此 IP 或 MAC 其中任何一个匹配均认为是此用户，此同步录入的用户属于静态绑定的用户，不会再进行其它方式的认证同时用户录入到本地后，可以针对此录入的用户组或用户进行相关功能的引用控制，比如：审计策略、控制策略、流控策略、限额策略等。SNMP 同步支持任务周期配置，即每经过任务周期的时间进行一次同步，支持配置时间为 2-36000 秒。
- ARP 扫描：通过 ARP 请求报文来获取内网 PC 的 IP 和 MAC 地址对应关系，同步下来的 IP 地址和 MAC 地址的对应关系可以录入到用户组也可以进行 IP-MAC 绑定。录入到用户组支持手工录入和自动录入，录入的用户以 IP 地址作为用户名，绑定其 IP 地址，此同步录入的用户属于静态绑定的用户，不会再进行其它方式的认证同时用户录入到本地后，可以针对此录入的用户组或用户进行相关功能的引用控制，比如：审计策略、控制策略、流控策略、限额策略等。ARP 扫描支持任务周期配置，即每经过任务周期的时间进行一次同步，支持配置时间为 10-36000 秒。由于 ARP 报文为二层报文，无法跨越三层网络，因此要求 ARP 扫描的网段必须是设备接口的直连网段。

1.2.2 用户同步流程

1. LDAP 同步用户流程

LDAP 同步主要是通过 LDAP 协议报文来获取配置的 Base DN 下的用户组织关系，以用户组（配置按 OU 同步时，即按照 LDAP 服务器上的 OU 来区分录入用户组配置，配置按安全组同步时，即 LDAP 服务器上的安全组来区分录入用户组配置）单元为单位，循环读取从 LDAP 服务器上发送回来的用户组及其包含的用户信息。

检查获取的用户组及用户数量是否到达或超过本地设备规格，若到达设备最大规格则将获取的信息丢弃结束同步过程，否则检查是否超过用户组用户最大规格，若超过则跳过此用户组单元，继续获取下一个用户组单元，直至获取完成或者到达设备规格；如不超过则将获取到的用户组及用户信息先保存到本地缓存中。

当一个用户组单元的信息获取完整后，将本地设备中同属于一个 LDAP 服务器的用户及用户组置 LDAP 标记，然后将获取的用户组单元信息其下发给 DPLAN 用以用户的认证以及设备本地用户的添加保存。在 DPLAN 保存用户及用户组时将已存在的用户及用户组的 LDAP 标记取消。

同步完成初始化同步标识等变量，释放已建立的会话，结束同步。

2. SNMP 同步流程

SNMP 同步主要是设备通过 SNMP 协议学习三层交换机上的 ARP 表，获得内网 PC 的 IP 和 MAC 对应关系，设备会通过 SNMP 报文去请求交换机上记录 ARP 表的 mib 节点来获取到其上面的 IP 与 MAC 的对应关系，然后根据配置选择是否自动录入到相应的用户组或者通过同步结果手工执行录入到用户组或 IP-MAC 绑定.。

- 交换机上已开启 SNMP 代理功能。
- 设备与交换机网络可达。
- 设备上配置的团体字与交换机团体字一致。

3. ARP 扫描流程

ARP 扫描主要通过 ARP 协议探测同网段主机地址，从而获取到内网 PC 的 IP 地址和 MAC 的对应关系。设备根据配置的扫描网段依次发送 ARP 请求报文，监听 ARP 回复报文来获取对应的 MAC 地址，然后根据配置选择是否自动录入到相应的用户组或者通过同步结果手工执行录入到用户组或 IP-MAC 绑定.。

ARP 扫描地址段必须是和设备同一网段.

1.3 配置用户同步

1.3.1 用户同步任务查看

在导航栏中选择“用户管理>用户管理>用户同步”，进入用户同步任务页面，可查看已配置的用户同步任务，如图 1-1 所示。

图1-1 用户同步任务列表

用户同步任务页面详细信息如表 1-1 所示

表1-1 用户同步任务列表详细信息表

标题项	说明
新建	新建任务
删除	批量删除任务
名称	任务名称
描述	任务描述
状态	任务状态 • 启用 • 禁用
同步类型	• LDAP 同步 • SNMP 同步 • ARP 扫描
同步周期	任务执行的周期
自动录入	是或者否
同步状态	任务执行状态结果，同步成功或者同步失败。
操作	立即同步，单击即可执行同步任务； 同步结果，单击显示同步结果； 编辑，单击进入任务编辑页面； 删除，删除同步任务。

1.3.2 配置 LDAP 同步

在导航栏中选择“用户管理>用户管理>用户同步”，单击<新建>按钮，选择<LDAP 同步>进入 LDAP 同步配置界面，如图 1-2 所示；LDAP 同步详细参数如表 1-2 所示。

图1-2 LDAP 同步配置界面

表1-2 LDAP 同步界面参数说明

参数	说明
名称	LDAP同步条目名称。
描述	LDAP同步描述信息。
LDAP服务器	选择引用的LDAP服务器。
同步类型	• 按 OU 同步：OU 同步 AD 域下 OU 用户； • 按安全组同步：安全组同步 AD 域下组用户。
自动同步	启用或禁用自动同步功能。
起始时间	LDAP同步条目创建后开始同步的时间。
间隔时间	LDAP同步条目创建后按照时间间隔进行同步。
用户组	LDAP用户同步到某一用户组

1.3.3 配置 SNMP 同步

1. 配置 SNMP 同步

在导航栏中选择“用户管理>用户管理>用户同步”，单击<新建>按钮，选择<SNMP 同步> 进入 SNMP 同步配置界面，如图 1-3 所示；SNMP 同步详细参数如表 1-3 所示。

图1-3 SNMP 同步配置界面

表1-3 SNMP 同步界面参数说明

参数	说明
启用	SNMP同步功能启用、禁用。
名称	SNMP同步条目名称。
描述	SNMP同步描述信息。
IP地址	交换机ip地址，需要与设备互通。
MAC地址	与设备相连的交换机接口的IP/MAC地址。
团体名	交换机启用SNMP功能所配置的团体字。
版本号	交换机SNMP版本号，支持V1、V2和V3。
任务周期	启用后按照所配置的时间进行SNMP用户同步。
自动录入	启用后同步用户录入设备可选指定用户组录入用户，不启用只同步不录入。

录入方式	默认录入：以IP地址作为录入名，绑定IP地址及MAC地址； IP录入：以IP地址作为录入名，只绑定IP地址； MAC录入：以MAC地址作为录入名，只绑定MAC地址。
IPMAC自动绑定	启用后，设备自动把第一次学到的IP/MAC进行唯一性绑定，无需手工绑定。

2. 配置用户 MAC 敏感

SNMP 同步场景下需要配合用户 MAC 敏感功能一起使用.

user mac-sensitive 命令用来配置用户识别是否对 MAC 变化保持敏感。

【命令】

user mac-sensitive｛**enable**｜**disable**｝

【视图】

(config)#视图

【参数】

enable：开启用户 MAC 敏感，用户 MAC 发生变化后会被踢下线重新识别。

disable：关闭用户 MAC 敏感。

【使用指导】

用户 MAC 敏感命令是配合 SNMP 跨三层学习 MAC 功能一起使用的，默认情况下为 disable 状态，即用户 MAC 发生变化后用户不会被踢下线；在跨三层环境下由于通过 SNMP 获取到真实 MAC 后在线用户的 MAC 会发生变化，开启 MAC 敏感以将用户踢下线，重新进行识别，以便重新关联用户。

说明：跨三层环境下，用户上线时 MAC 识别为匿名用户，MAC 地址为下联三层设备的接口 MAC1，用户静态绑定条目为（user2 MAC2），当开启跨三层学习后，正常获取到用户的真实 MAC2,如果用户 MAC 敏感为关闭状态，用户不会重新识别会导致无法关联上静态绑定用户，在线用户仍然会显示匿名用户，就会导致所有引用了账号 user2 的策略均不生效。

【举例】

配置用户 MAC 敏感

```
Host(config)# user mac-sensitive enable   开启用户 MAC 敏感
Host (config)# user mac-sensitive disable   关闭用户 MAC 敏感
```

1.3.4 配置 ARP 扫描

在导航栏中选择“用户管理>用户管理>用户同步”，单击<新建>按钮，选择<ARP 扫描> 进入 ARP 扫描配置界面，如图 1-4 所示；ARP 扫描详细参数如表 1-4 所示。

图1-4 ARP 扫描配置界面

表1-4 ARP 扫描界面参数说明

参数	说明
启用	ARP扫描功能启用、禁用。
名称	ARP扫描条目名称。
描述	ARP扫描描述信息。
扫描网段	需要和设备是同一网段，例如接口192.168.1.1/24，扫描需要配置成192.168.1.0/24。
任务周期	启用后按照所配置的时间进行ARP扫描同步。
自动录入	启用后同步用户录入设备可选指定用户组录入用户，不启用只同步不录入。
IPMAC自动绑定	启用后，设备自动把第一次学到的IP/MAC进行唯一性绑定，无需手工绑定。

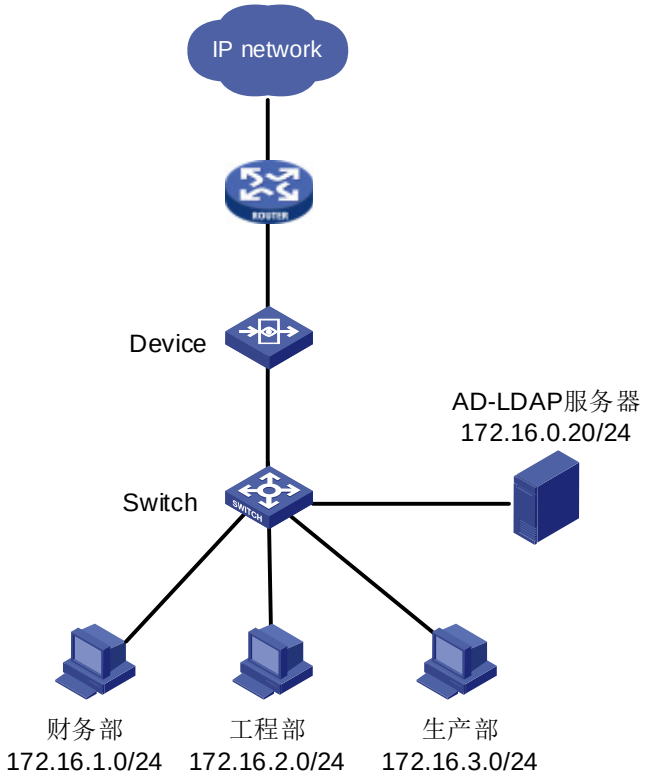
1.4 用户同步配置举例

1.4.1 组网需求

如图 1-5 所示，某公司的财务部、工程部员工通过固定设备使用静态绑定 IP/MAC 的方式上网，生产部员工使用 LDAP 服务器配置的用户账号认证上网，其网段分别是 172.16.1.0/24、172.16.2.0/24 和 172.

16.3.0/24，LDAP 服务器的地址为 172.16.0.20/24。工程部 SNMP 交换机地址为 172.16.0.10/24。使用设备的 ge0 和 ge1 接口，以透明模式部署在网络中，在设备上配置用户同步。

图1-5 用户同步配置举例组网图



1.4.2 配置步骤

1. 添加 LDAP 服务器

通过菜单“用户管理>认证管理>认证服务器”，单击选择“新建>LDAP 服务器”，进入如图 1-6 所示的页面。

图1-6 LDAP 服务器配置

2. 配置用户组

通过菜单“用户管理>用户组织结构”，单击选择“新建>用户组”，配置财务部和工程部用户组，如图 1-7、图 1-8 所示。

图1-7 财务部用户组配置

图1-8 工程部用户组配置

3. 配置用户同步认证

(1) 配置 LDAP 同步

通过菜单“用户管理>用户管理>用户同步”，单击选择“新建>LDAP 同步”，进入 LDAP 同步配置页面。配置 LDAP 同步任务名称，选择 LDAP 服务器，选择开启同步周期并配置同步周期（每天的某个整点），或者选择关闭周期同步，如图 1-9 所示。

图1-9 配置生产部 LDAP 同步

(2) 配置 SNMP 同步

通过菜单“用户管理>用户管理>用户同步”，单击选择“新建>SNMP 同步”，进入 SNMP 配置页面。配置 SNMP 同步任务名称，IP 地址和 MAC 地址配置为 SNMP server 的 IP 地址和 MAC 地址，配置团体名和 SNMP 的版本号，选择开启周期同步并配置同步周期或者关闭周期同步（只在配置成功后同步一次），选择开启自动录入并配置同步结果的录入用户组，或者关闭自动录入由后期用户手动添加。如图 1-10 所示。

图1-10 配置工程部 SNMP 同步

(3) 配置 ARP 扫描

通过菜单“用户管理>用户管理>用户同步”，单击选择“新建>ARP 扫描”，进入 ARP 扫描配置页面。配置“扫描网段”为财务部网段，选择配置是否开启周期同步，是否开启自动录入并选择录入用户的组织结构的用户组。如图 1-11 所示。

图1-11 配置财务部 ARP 扫描

4. 配置用户认证地址对象

通过菜单“策略配置>对象管理 > 地址对象 > IPv4 地址对象”，单击<新建>按钮，配置生产部地址对象，如图 1-12 所示。

图1-12 地址对象配置

5. 配置 Web 认证参数

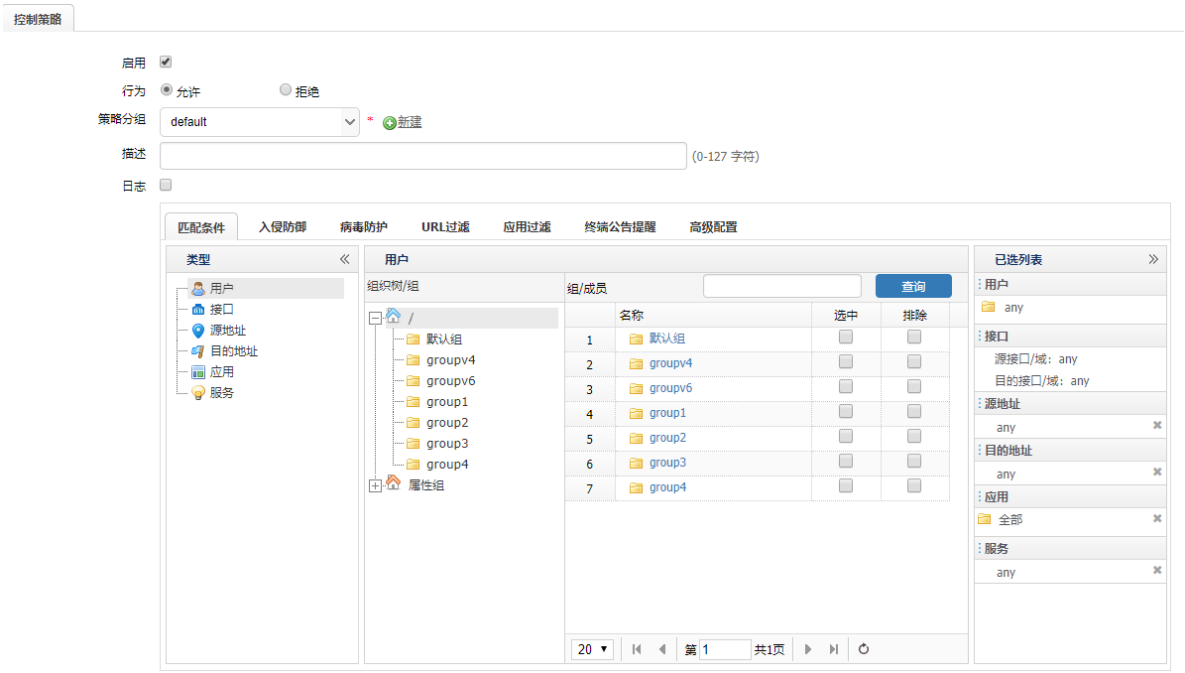
通过菜单“用户管理 > 认证管理 > 认证方式 > 本地 WEB 认证”，勾选“允许重复登录”，配置“允许登录数”为无限制，单击<提交>。如图 1-13 所示。

图1-13 配置 Web 认证

6. 配置安全策略

通过菜单“策略配置>控制策略”，单击<新建>按钮进入控制策略配置界面。如图 1-14 所示。

图1-14 控制策略配置



7. 全局配置启用第三方认证选择 LDAP 服务器

在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证，选择 LDAP 服务器，如图 1-15 所示。

图1-15 全局模式启用第三方 Ldap 配置

8. 配置用户策略

通过菜单进入“用户管理>认证管理>认证策略”，单击<新建>，源地址配置为“生产部地址对象”，认证方式配置为“Web 认证”，其它选项保持默认，单击<提交>。如图 1-16 所示。

图1-16 用户策略配置

1.4.3 验证配置

(1) 进入“用户管理>用户组织结构”，查看“财务部”用户组。财务部 ARP 同步成功后，财务部固定设备的用户全部自动录入，用户静态绑定对应的 IP，固定设备直接可以上网。如图 1-17 所示。

图1-17 财务部 ARP 同步用户

(2) 进入“用户管理>用户组织结构”，查看“工程部”用户组。工程部 SNMP 同步成功后，生产部固定设备的用户全部自动录入，用户静态绑定对应的 IP/MAC，固定设备直接可以上网。如图 1-18 所示。

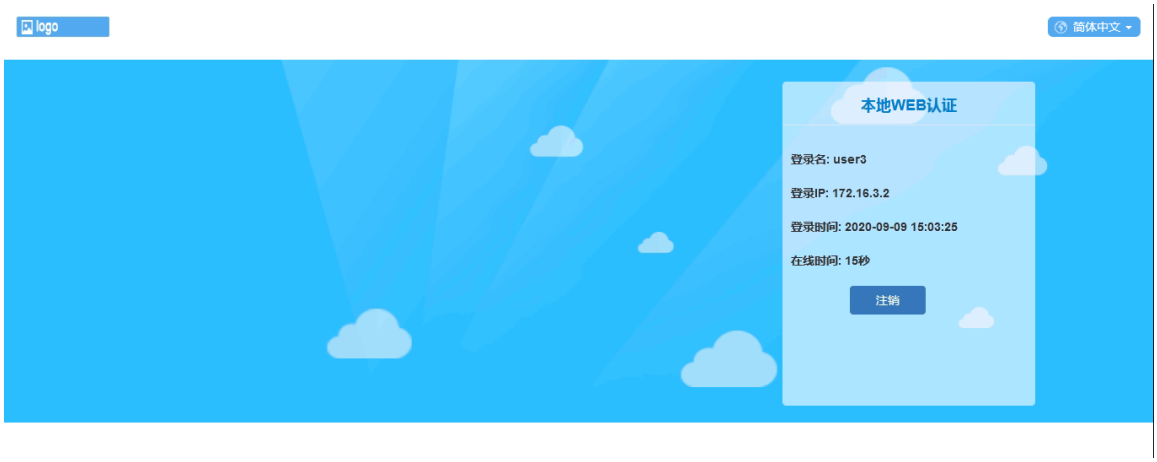
图1-18 工程部 SNMP 同步用户

(3) 进入“用户管理>用户组织结构”，查看“生产部”用户组。从 LDAP 成功同步了生产部的用户，同步了用户组“生产部”以及用户组的直属用户 user1，user2，user3。如图 1-19 所示。

图1-19 生产部 LDAP 同步用户

(4) 在生产部网段（172.16.3.0/24）使用 PC 终端进行 HTTP 访问，弹出本地 Web 认证页面，使用 LDAP 联动用户 user3 认证成功。如图 1-20 所示。

图1-20 生产部 LDAP 用户认证页面



目 录

1 单点登录 ····· 1-1
1.1 概述 ····· 1-1
1.1.1 原理描述 ····· 1-1
1.2 配置 AD 域单点登录 ····· 1-1
1.3 配置单点登录认证策略 ····· 1-3
1.4 配置 AD 域服务器 ····· 1-4
1.4.2 格式 1 ····· 1-7
1.4.3 格式 2 ····· 1-7
1.5 AD 域服务器上安装 ssoserver_setup.exe（可选） ····· 1-8
1.5.1 ssoserver_setup.exe 程序安装 ····· 1-8
1.5.2 www.sso.pub 域名配置 ····· 1-13
1.6 使用限制及注意事项 ····· 1-19

1 单点登录

1.1 概述

单点登录全称 Single Sign On（以下简称 SSO），是指在多系统应用群中登录一个系统，便可在其它系统中得到授权而无需再次登录，包括单点登录与单点注销两部分。

AD 域单点登录功能是指用户通过登录 AD 域服务器，实现 windows 登录和上网的账号认证。当用户通过域账号登录到某个 AD 域后，不需要再输入账号密码，自动通过设备的上网认证，实现单点登录功能。

1.1.1 原理描述

- AD 域服务器配置组策略，加载 sso_setup.exe 脚本（登录脚本），当用户以域账号正常登录 AD 域服务器时，获取到相应组策略，执行 sso_setup.exe 脚本向网关发送认证登录报文；当域用户从域中注销时，执行 sso_setup.exe 脚本向网关发送注销报文，AD 域服务器首次配置完成后，整个认证登录、注销过程都不需要用户参与。
- 网关监听指定的 udp 端口，接收域用户通过登录脚本发送的域用户单点登录信息。
- 登录报文加密传输，且可防止回放攻击。
- 网关设备收到登录报文后，对报文信息进行校验，校验通过后对用户执行登录操作，若收到退出报文，则对用户执行注销操作。

单点登录配置、登录流程如下：

(1) 域管理员配置 AD 域服务器，加载用户上下线时需执行的脚本程序。

(2) 网关开启单点登录功能，配置通信密钥，配置单点登录认证策略。

(3) 域用户成功登录域服务器，执行登录脚本，向网关发送认证消息。

(4) 网关收到认证报文后，自动完成用户上网认证；收到注销报文，自动完成用户注销。

1.2 配置AD域单点登录

在导航栏中选择“用户管理 > 认证管理 > 认证方式 > 单点登录”，进入单点登录全局参数配置页面，如图 1-1 所示

图1-1 单点登录全局参数配置页面

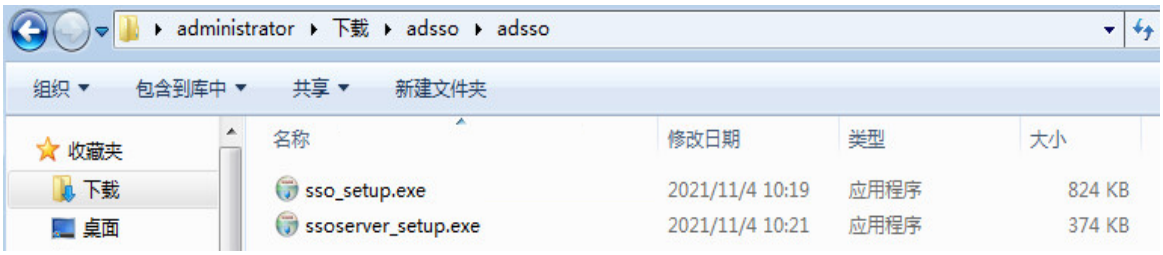
单点登录全局配置参数详细说明，如表 1-1 所示

表1-1 全局配置参数详细说明

标题	说明
启用	单点登录启用或禁用，默认未启用。
单点登录程序	单点登录程序用于AD域服务器配置登录脚本，包括sso_setup.exe和ssoserver_setup.exe两个应用程序； sso_setup.exe应用程序：主要在域PC登录时通过AD域服务器下发自动安装，安装成功之后给设备发送指定的上下线报文的信息。 ssoserver_setup.exe应用程序：ssoserver为一个下载单点登录程序安装包的http/https服务器，此程序可根据实际需要安装，当域PC与AD域服务器通信出现异常无法通过域服务器自动安装sso_setup.exe程序时，可以安装ssoserver_setup.exe程序，将sso_setup.exe程序放到ssoserver程序安装的目录下，并在ssoserver安装目录下配置好对应的sso.ini文件，域PC通过访问http://www.sso.pub:880/sso_setup.exe下载程序手动安装，程序手动安装之后会通过8443端口自动到ssoserver上获取sso.ini文件里的配置信息。
会话密钥	网关配置密钥，与AD域服务器上脚本参数或者sso.ini文件里密钥配置保持一致，长度为1-31个字符，不允许输入字符<>+\^"?和空格。

单击“下载域单点登录程序”下载单点登录脚本文件，下载完成后的压缩包内文件如图 1-2 所示。

图1-2 单点登录程序压缩包文件



1.3 配置单点登录认证策略

在导航栏中选择“用户管理 > 认证管理 > 认证策略”，进入认证策略显示页面，单击“新建”按钮，进入认证策略配置页面，如图 1-3 所示，认证方式选择单点登录。

图1-3 认证策略配置页面

单点登录用户策略配置参数说明，如表 1-2 所示。

表1-2 单点登录用户策略配置详细说明

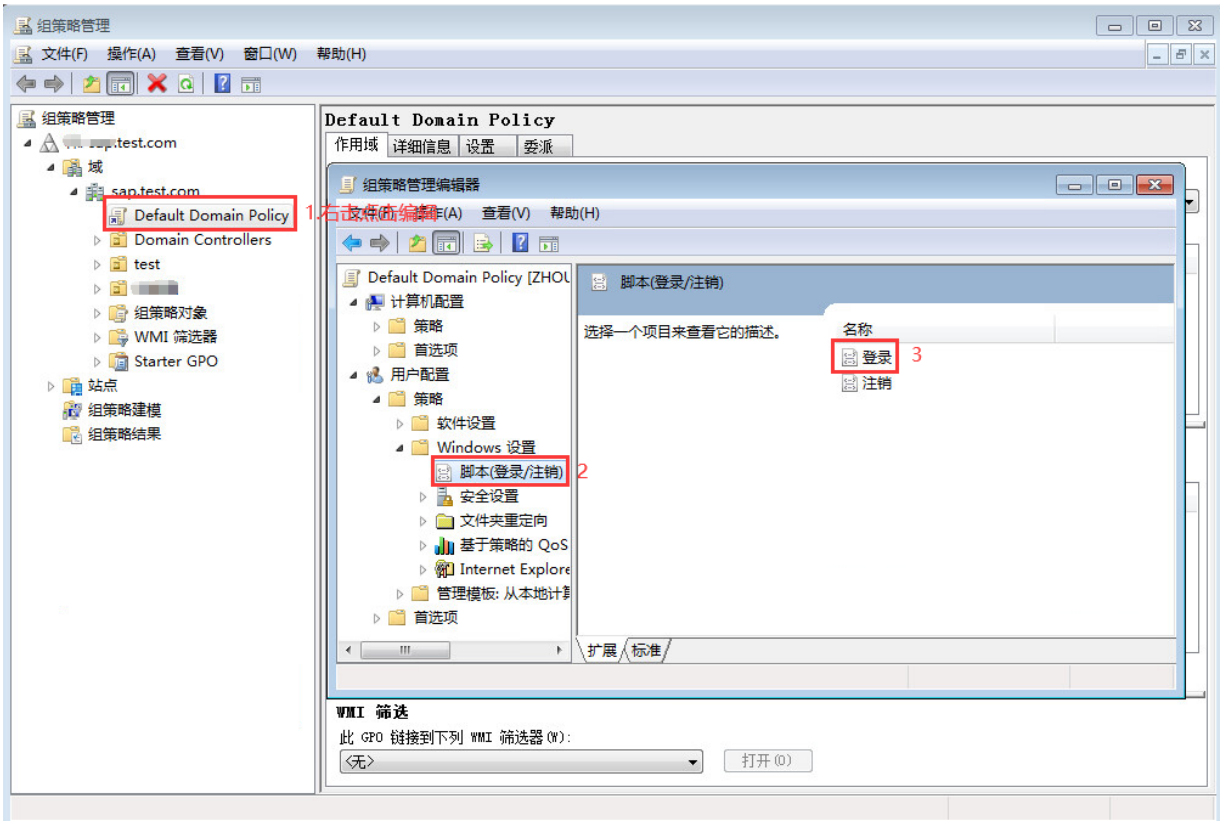
参数	说明
源接口	单点登录用户的接口。
源地址	单点登录用户的IP范围。

参数	说明
认证方式	可以选择多种认证方式，如图可配置单点登录认证策略，当用户认证失败时，以下两种处理方案供用户选择： 不需要认证，用户直接上线。 跳过当前这条认证策略，匹配后面的策略。
时间	认证策略时间对象，时间对象有效期内策略生效，时间对象无效的时候认证策略为禁用状态。
用户录入	默认不选择用户组，第三方用户认证成功后不录入用户；选择用户组后，第三方用户认证成功后录入指定的用户组。
用户有效时间	用户有效期指的是第三方用户录入方式： • 永久录入：第三方用户认证成功后录入指定组，永久有效。 • 有效期至：第三方用户认证成功后录入指定组，设备运行时间到配置的时间当天23:59后，录入的用户状态变为不启用，认证策略也变为不启用。 临时录入：第三方用户认证成功后录入指定组，用户注销下线后，录入的用户组里用户自动删除。

1.4 配置AD域服务器

进入组策略：以 windows 2008 server 为例，登录到 AD 域服务器，“运行”中输入 gpmc.msc。选择“Default Domian Policy > 用户配置 > 脚本（登录）”, 如图 1-4 所示。

图1-4 组策略管理



双击“登录”选项，选择“显示文件”，将下载的 sso_setup.exe 文件拷贝到此目录。

图1-5 登录脚本设置

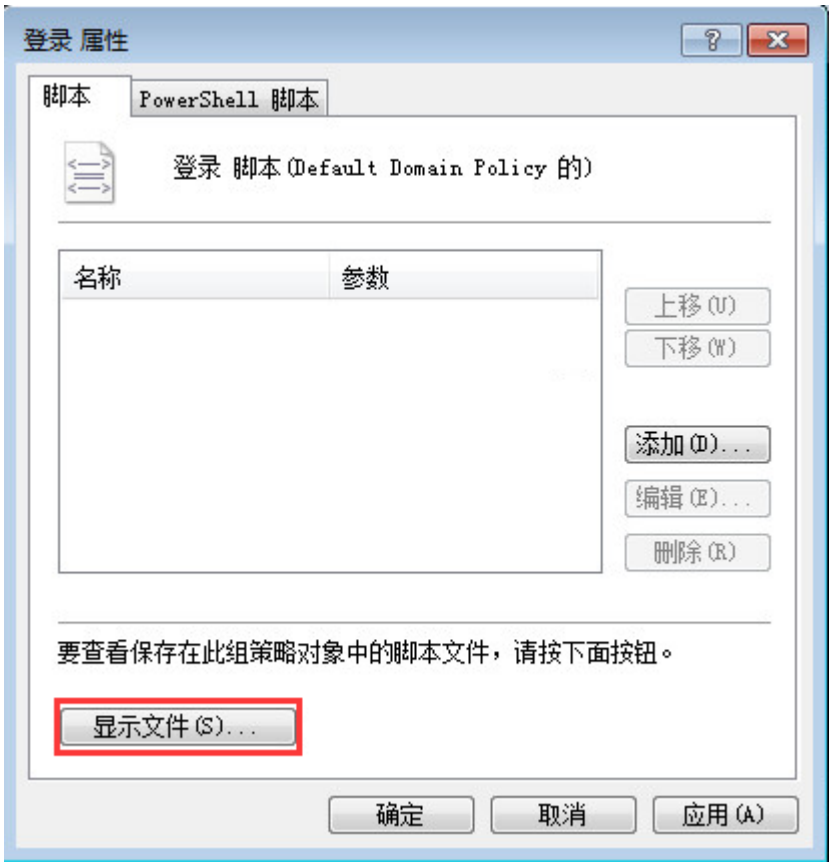
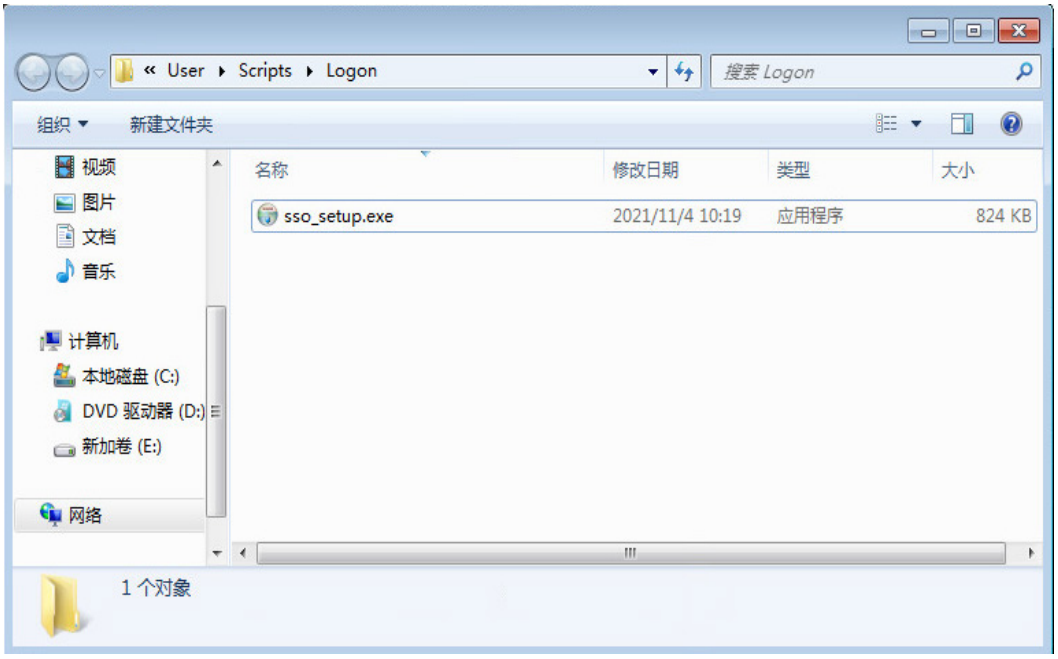


图1-6 显示文件



返回“登录”属性窗口，单击“添加”，在弹出的窗口中设置脚本名以及脚本参数，脚本参数有以下两种配置方式。

1.4.2 格式 1

以“/S Value1 Value 2 Value 3”的形式包含四个参数，参数间以空格隔开，四个参数缺一不可，其中：

- /S：代表程序静默安装（即自动安装），必须大写；
- Value 1：代表内网用户可访问到的设备网口 IP；
- Value 2：代表设备监听端口（固定为 6622，不可改变）；
- Value 3：代表通信密钥（必须同设备侧单点登录全局参数设置的密钥统一）。

图1-7 配置脚本（4 个参数）

1.4.3 格式 2

以“/S Title1=value1 Title 2=value2 …… Title15=value15”的形式包含多个参数，参数间以空格隔开，且参数的 Title 部分建议都大写。

图1-8 脚本配置（多个参数）

目前支持的参数有如下项：

- /S：表示静默安装单点登录程序；
- IP=192.168.1.1 ：代表设备地址；
- PORT=6622 ：代表设备监听端口；

- KEY=admin.123 ：代表域 PC 与设备之间的通信密钥，与设备端配置需要保持一致；
- HB=1：代表心跳开关，默认开启，0 表示关闭；
- HBI=30 ：代表心跳时间间隔，默认 30，单位秒，范围 30-600 之间的正整数；
- UDI=30 ：代表配置更新时间间隔以及配置更新开关，不配置表示关闭，配置表示打开，默认 30，单位秒，范围 30-600 之间的正整数。

更新组策略，为了使用更改的组策略立即生效，需要刷新组策略，刷新组策略命令为 **gpupdate.exe** 刷新组策略后，域用户重新上线，即可生效。

1.5 AD域服务器上安装ssoserver_setup.exe（可选）

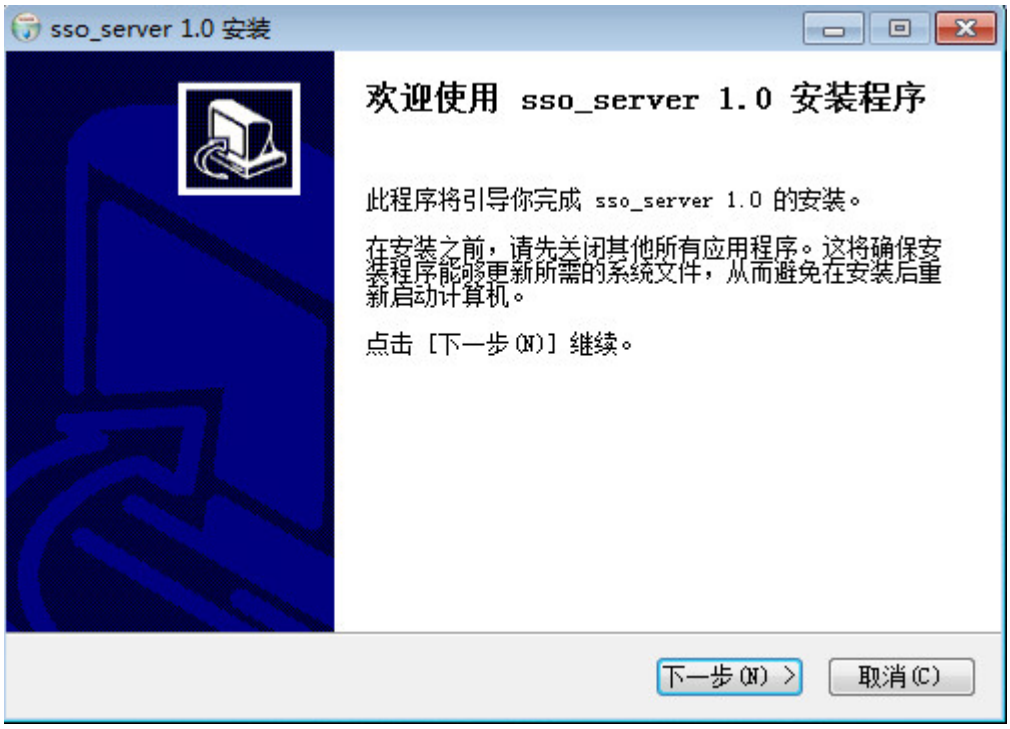
当域 PC 加入 AD 域服务器后，如果与服务器通信异常时，无法通过 AD 域脚本参数推送单点登录程序自动安装，则需要通过其他方式下载单点登录程序客户端到域 PC 上安装。

- **方法一：**可以直接通过设备上下载单点登录程序（但此项仅管理员有操作权限，普通用户无登录设备权限，普通用户只能通过管理员提供的单点登录程序安装）在域 PC 上安装，域 PC 上安装之后还需要将加密的配置文件（sso.ini）拷贝到 sso_setup.exe 程序安装的目录下，用户才可上线；
- **方法二：**安装 ssoserver_setup.exe 程序，此程序安装之后拥有 http 和 https 方式下载服务，将 sso_setup.exe 程序放到 ssoserver_setup.exe 安装目录下，并在安装目录下配置好对应的 sso.ini 文件，域 PC 通过 http://www.sso.pub:880/sso_setup.exe 下载登录脚本程序手动安装，安装完之后域 PC 会通过 https 的 8443 端口自动到 ssoserver 上获取 sso.ini 文件。

1.5.1 ssoserver_setup.exe 程序安装

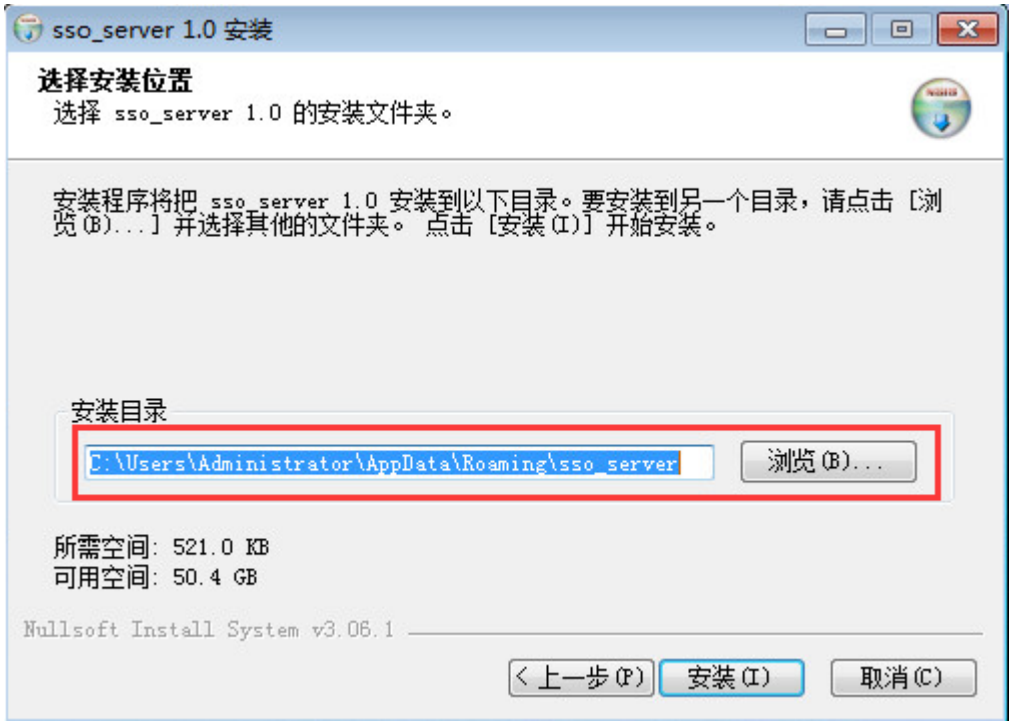
(1) 双击 ssoserver_setup.exe 程序，安装前建议先将 360 安全软件退出再安装（原因是安装程序会设置开启自启动 360 安全软件会误阻断导致程序无法启动），点击安装，默认点击下一步。

图1-9 ssoserver 程序安装



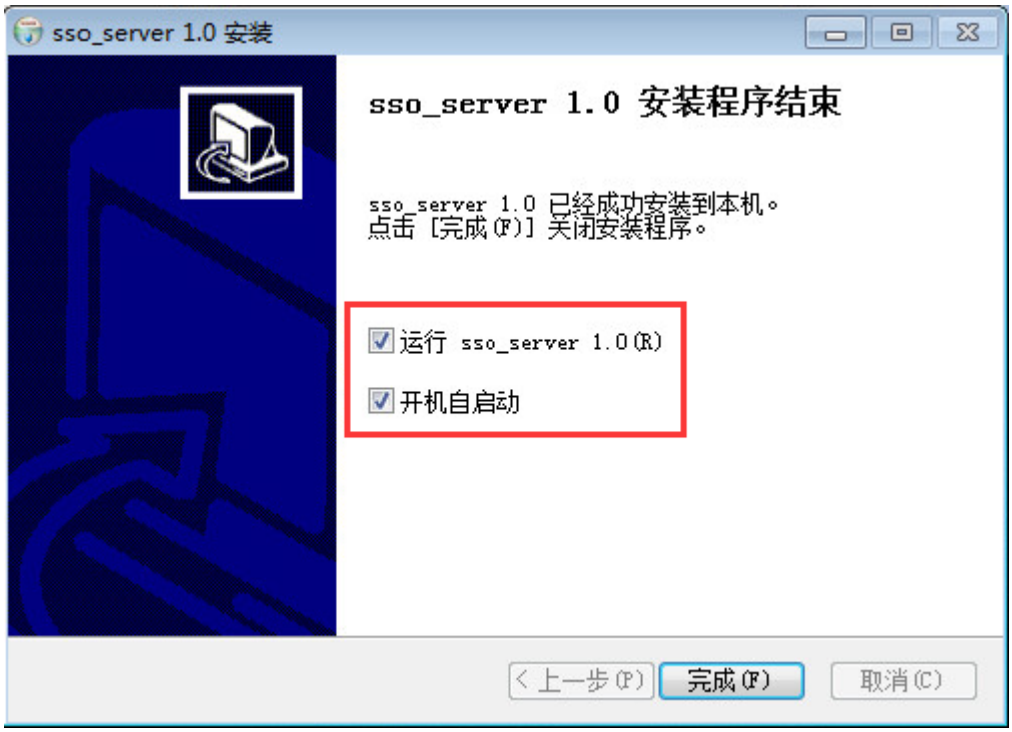
(2) 点击下一步，安装目录默认 C 盘（“C:\Users\Administrator\AppData\Roaming\sso_server”），也可指定到其他安装目录，此处需要记录一下对应的安装目录，便于安装完之后配置 sso.ini 文件和存放 sso_setup.exe 程序需要到此安装目录。

图1-10 ssoserver 程序安装目录



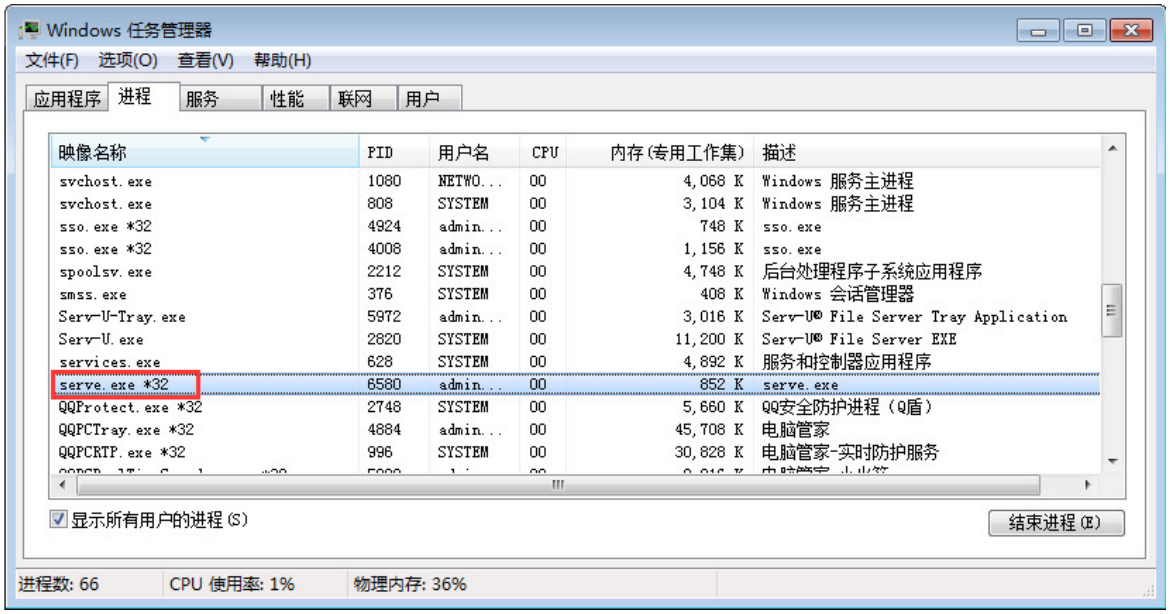
(3) 点击安装，安装完成之后默认勾选“运行 sso_server”和“开启自启动”，此选项不用修改，如果取消勾选，则程序不会自动运行，需要到安装目录去手动启用。点击“完成”安装，ssoserver 安装完成。

图1-11 ssoserver 程序安装完成



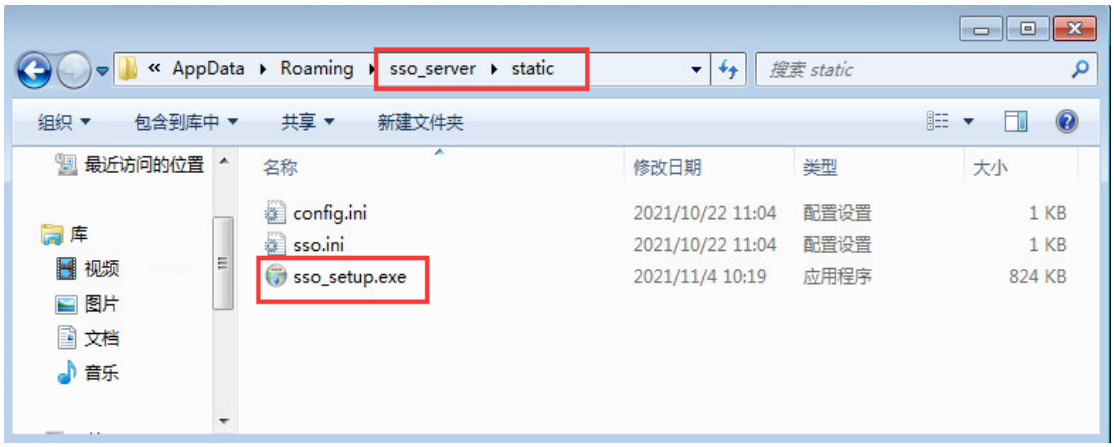
(4) 安装完成后可以在任务管理器里查看到 serve.exe 进程，表示 ssoserver 程序已运行。

图1-12 任务管理查看 ssoserver 程序进程



(5) 进入到 ssoserver 安装目录下（“C:\Users\Administrator\AppData\Roaming\sso_server”），将 sso_setup.exe 拷贝到如下目录。

图1-13 sso_setup.exe 程序拷贝到 ssoserver 程序安装目录



(6) 在该目录下双击打开 sso.ini 文件，修改配置文件里的 GWIP（设备的 IP 地址）和 SessionKey（与设备单点登录会话密钥配置一致）信息，其他参数不用修改，并保存。

图1-14 修改 ssoserver 安装目录下 sso.ini 文件

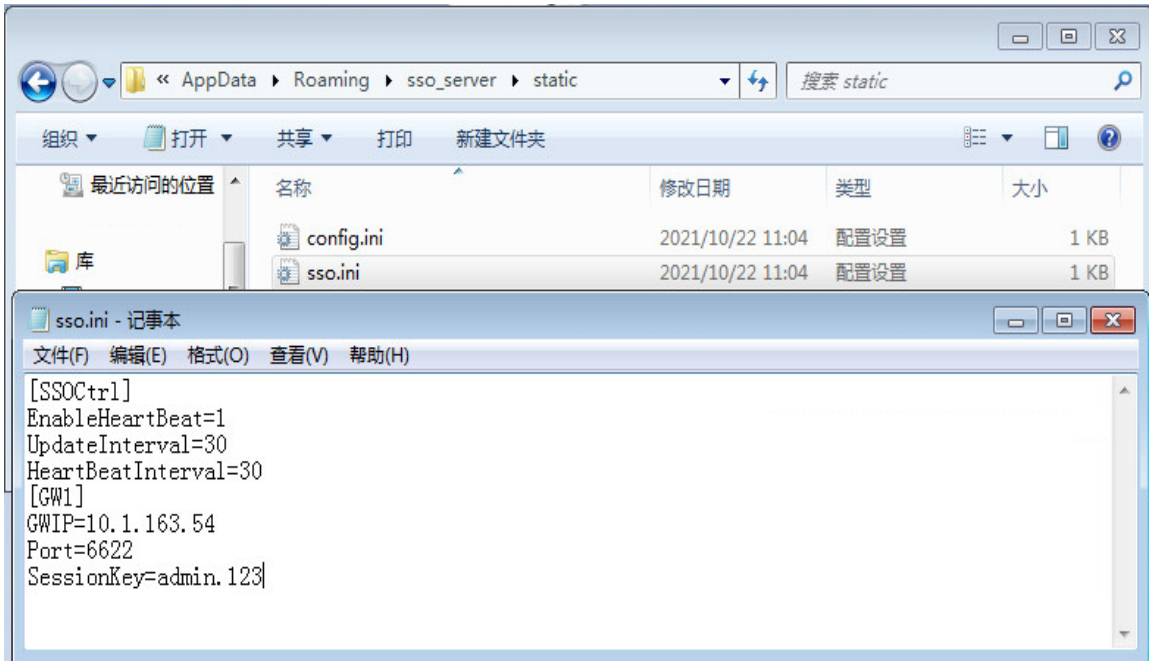


表1-3 sso.ini 配置文件参数说明

参数	说明
EnableHeartBeat	是否启动心跳功能（0：关闭 ， 1：开启），默认为1开启状态
UpdateInterval	配置更新时间间隔，单位秒，默认30s，范围是30-600之间的正整数

HeartBeatInterval	发送心跳的时间间隔（正整数，范围[30, 600]，默认值：30）
GWIP	网关的IP
SessionKey	会话密钥（大小写敏感、支持特殊字符，最长32个字符）
Port	端口号（6622，不能改变）

Ssoserver 安装目录下还有一个 config.ini 文件，此文件用来更新 sso_setup.exe 程序。

图1-15 ssoserver 安装目录下 config.ini 文件

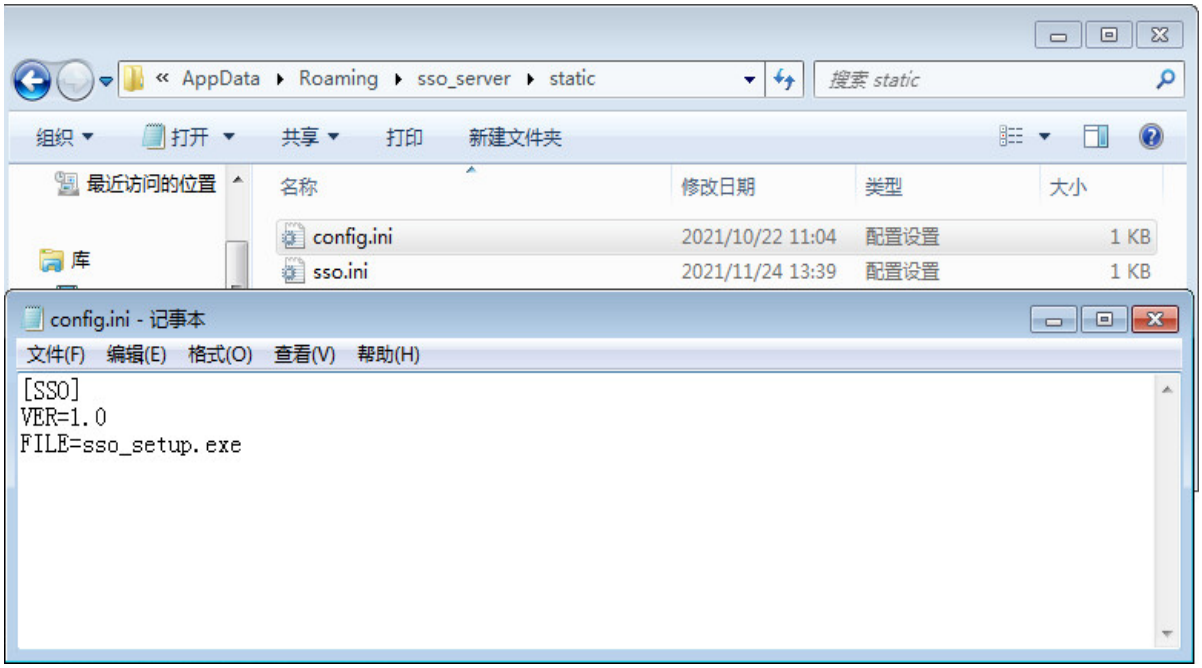


表1-4 config.ini 配置文件参数说明

参数	说明
VER	代表sso_setup.exe的版本号，首次发布版本号为1.0，如果后续sso_setup.exe程序有更新，可以将程序版本号进行修改，并将对应程序放到此目录下。
FILE	sso_setup.exe程序名称，此名称不支持修改，修改后下发给客户端会导致安装失败。

说明

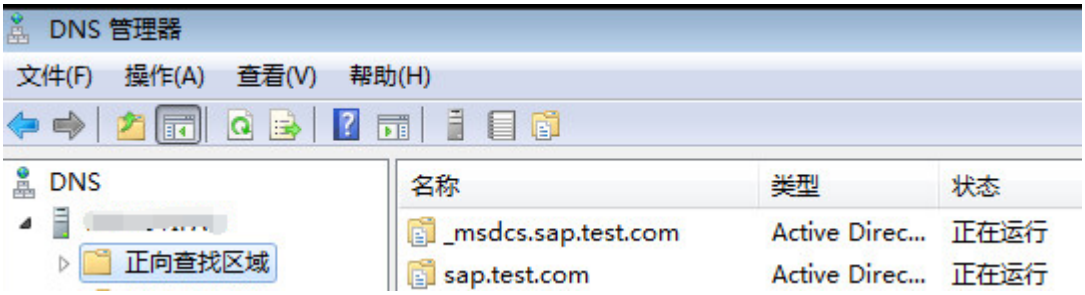
如果 AD 服务器有安全软件或开启了自带的防火墙，需要放通 TCP 的 880 和 8443 端口。因为 PC 使用 880 端口下载单点登录程序，单点登录程序安装后通过 8443 端口获取 sso.ini 文件中的配置参数。

1.5.2 www.sso.pub 域名配置

ssoserver_setup.exe 程序安装完之后，还需要配置 DNS 域名信息，具体配置如下：

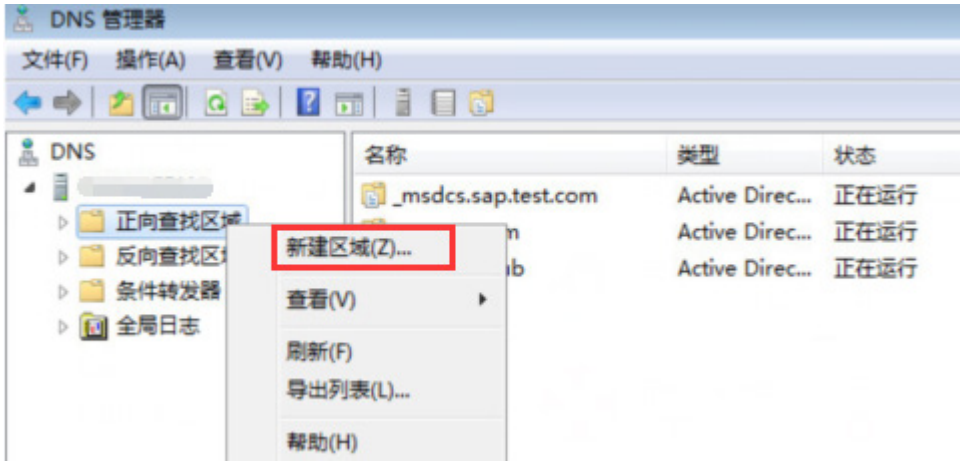
(1) AD 域服务器“开始菜单>管理工具>DNS”，打开 DNS 管理页面。

图1-16 DNS 管理页面



(2) 在“正向查找区域”点右键，选择“新建区域”打开新建区域向导。

图1-17 右击新建区域

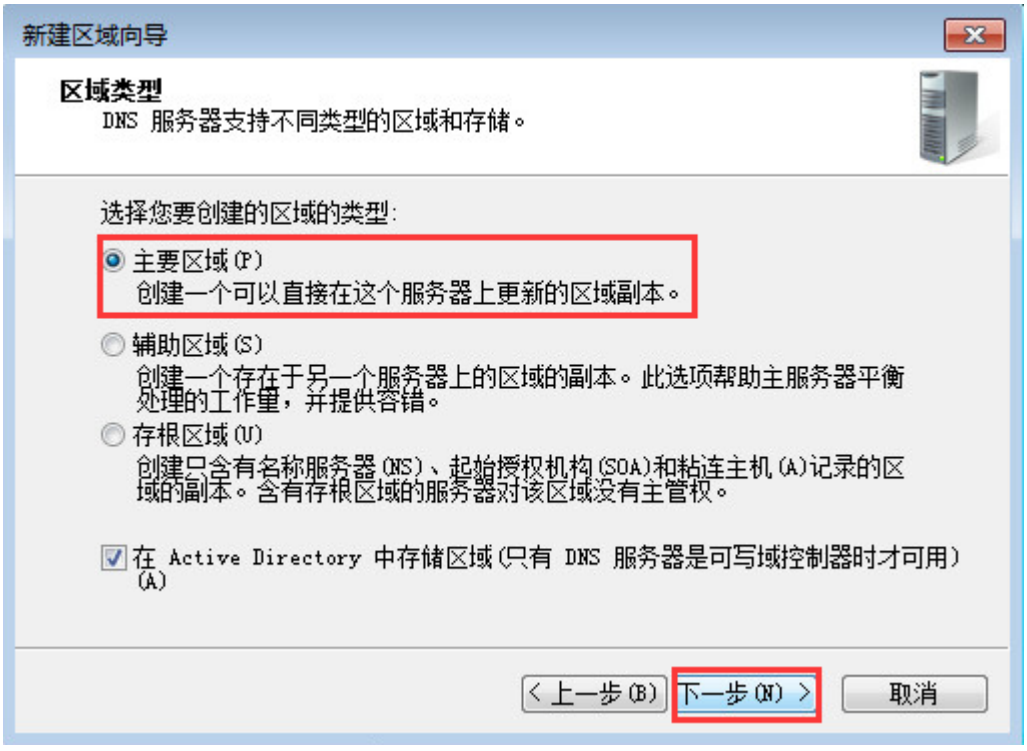


(3) 新建区域向导，点击“下一步”。

图1-18 新建区域向导

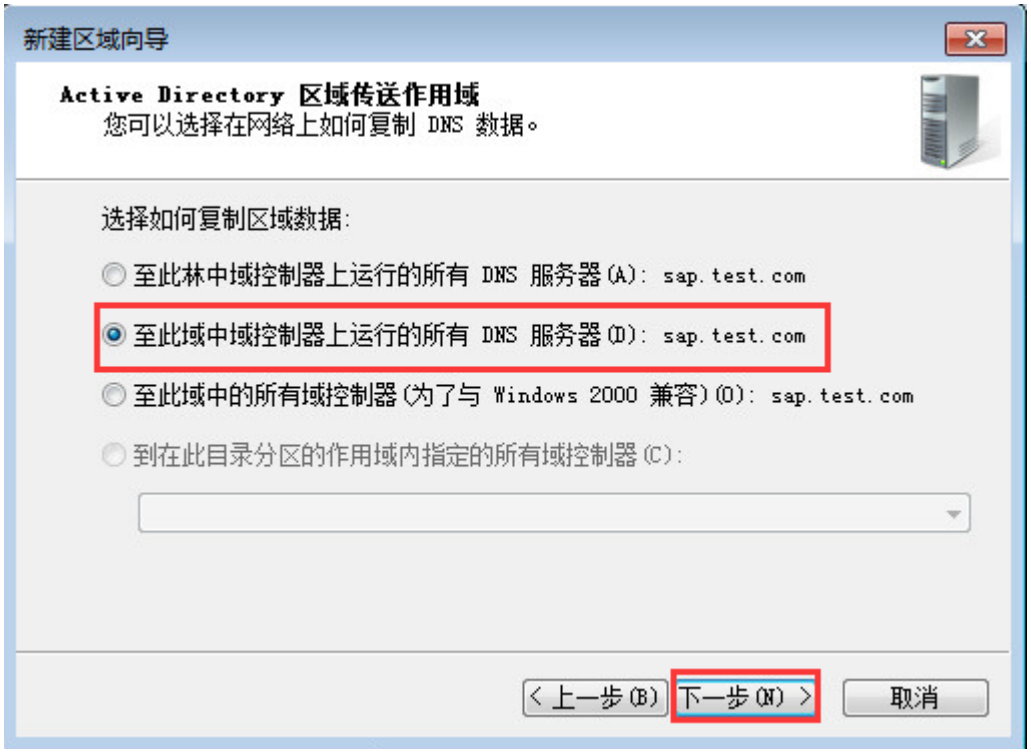
(4) 区域类型选择主要区域，点击“下一步”。

图1-19 区域类型



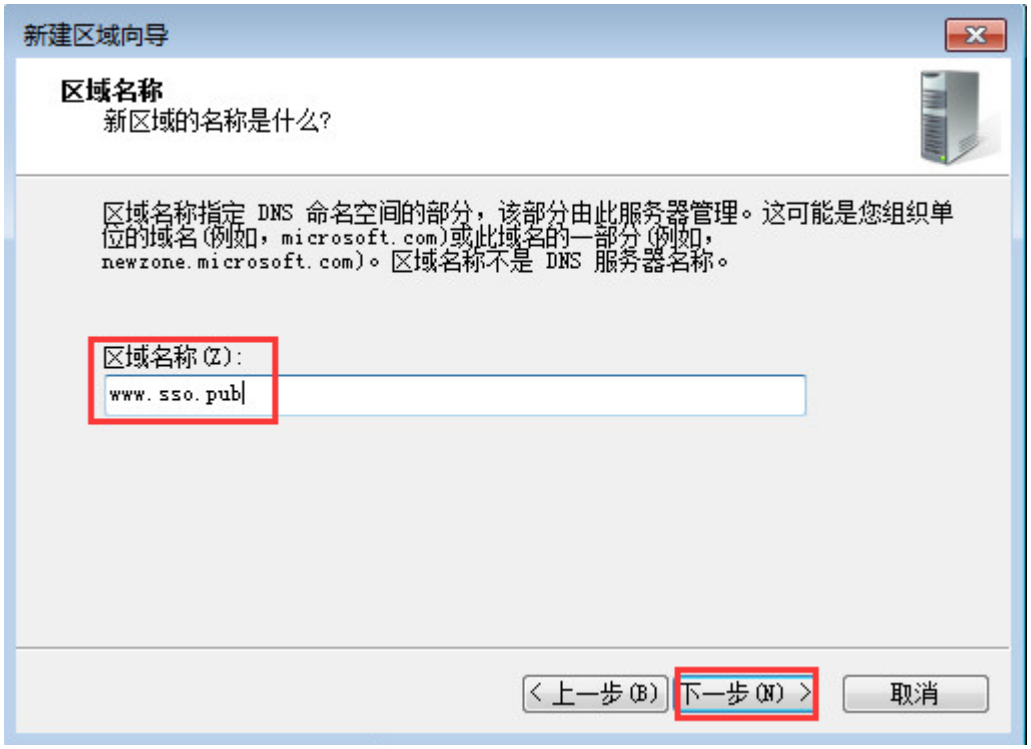
(5) Active Directory 区域传送作用域，点击“下一步”。

图1-20 区域传送作用域



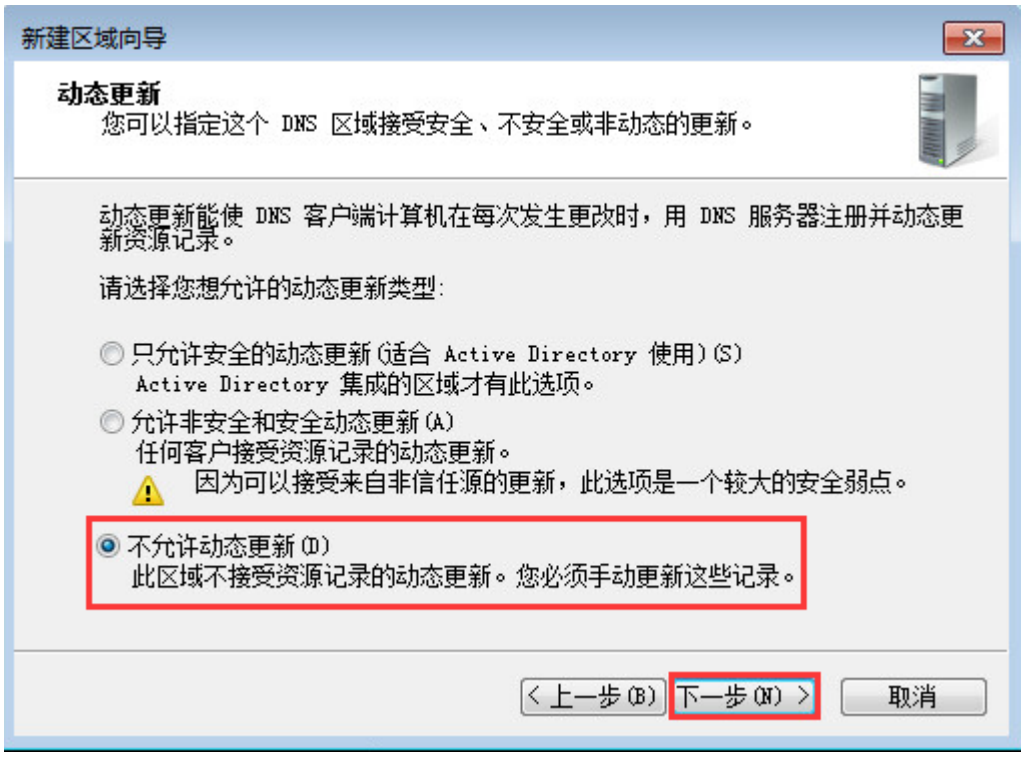
(6) 区域名称配置为“www.sso.pub”，点击“下一步”。

图1-21 区域名称配置



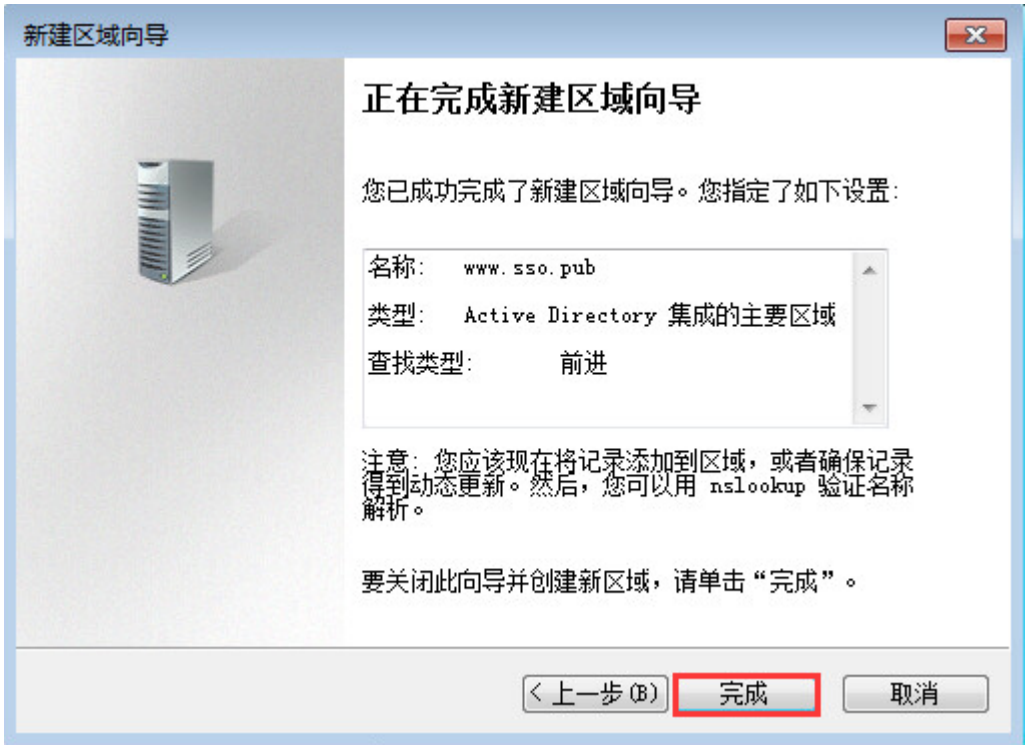
(7) 动态更新选择“不允许动态更新”，点击“下一步”。

图1-22 动态更新



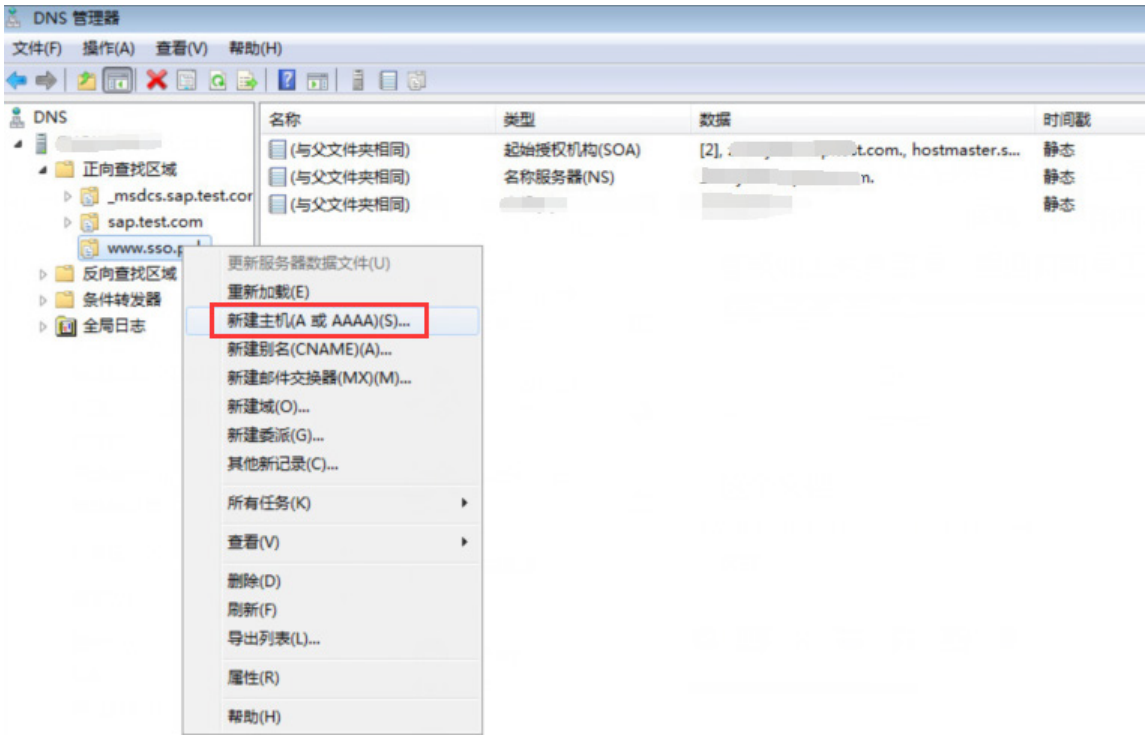
正在完成新建区域向导，点击“完成”。

图1-23 新建区域配置完成



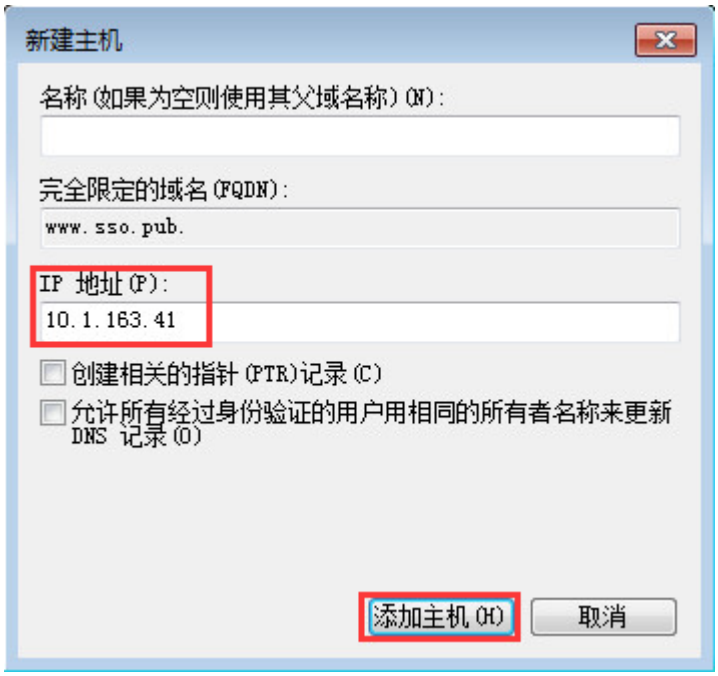
(8) DNS管理界面展开“正向查找区域>wwww.sso.pub”，在右侧空白处点击右键，选择“新建主机”。

图1-24 右击新建主机



(9) 弹出新建主机配置界面，IP 地址配置为“10.1.163.41”即安装 ssoserver 这台服务器的 IP 地址（也就是 AD 域服务器地址），点击 “添加主机”。

图1-25 添加主机地址



点击“确定”后并点击“完成”，主机记录配置完成。

图1-26 点击确定

图1-27 点击完成

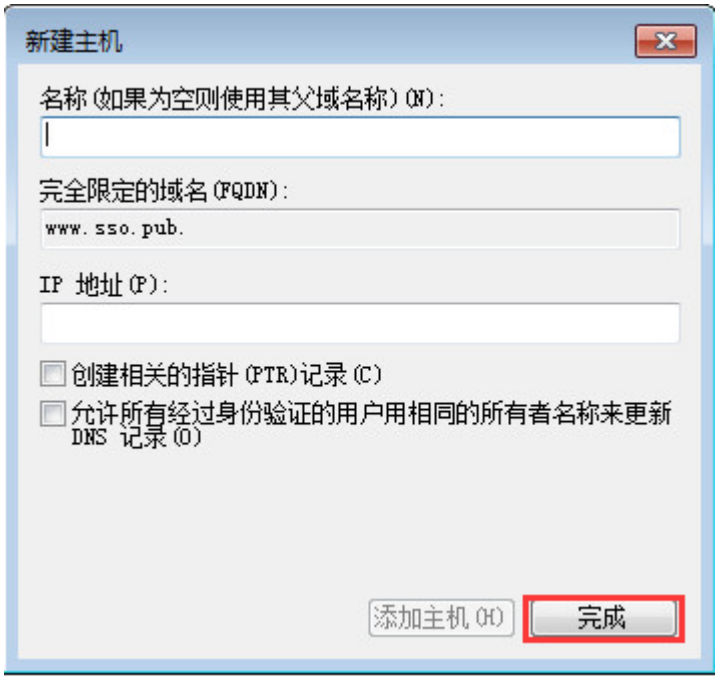


图1-28 配置完成后查看 www.sso.pub 主机地址

至此 ssoserver_setup.exe 所有配置完成。

域 pc 可通过 http://www.sso.pub:880/sso_setup.exe 下载单点登录程序包进行手动安装，如果无法访问，请检查 AD 域服务器上防火墙是否放通了 880 和 8443 端口。

1.6 使用限制及注意事项

- 单点登录功能目前仅支持 AD 域系统，不支持其他系统。
- 支持的 AD 域服务器有 Windows 2003 server、Windows 2008 server、Windows 2012 server、Windows 2016 server、Windows 2019 server。
- 由于 sso_setup.exe 和 ssoserver_setup.exe 程序安装会在系统上添加自启动项，通过主流安全软件扫描有可能会被误阻断的现象，安装时需关注此项，如出现误阻断需要在杀毒软件上添加允许程序操作安装成功，如果 ssoserver_setup.exe 程序安装设置允许程序操作时，程序进程还是会被阻断的情况，导致 ssoserver 的 serve 进程被隐藏无法启动，此时重新安装也无法启动 serve 进程（出现此情况卸载 ssoserver 程序然后重启服务器，将 360 安全软件退出再重新安装），最好是将 360 安全软件退出安装程序。
- sso_setup.exe 和 ssoserver_setup.exe 程序下载安装会受杀毒软件扫描（目前程序已提交微软、360 杀毒、腾讯管家主流杀毒软件扫描，但是并不能完全保证杀毒软件不误识别的情况），杀毒软件有可能存在误识别病毒或木马的情况，如果存在此情况可先退出杀毒软件下载或者将软件添加信任。

目 录

1 对象管理 ····· 1-1
1.1 关键字对象 ····· 1-1
1.1.1 关键字对象简介 ····· 1-1
1.1.2 关键字列表配置 ····· 1-1
1.2 URL 对象 ····· 1-2
1.2.1 URL 过滤简介 ····· 1-2
1.2.2 配置 URL 分类 ····· 1-2
1.2.3 配置自定义 URL ····· 1-3
1.2.4 配置恶意 URL ····· 1-4
1.2.5 配置 URL 白名单 ····· 1-5
1.2.6 配置 HTTPS 对象 ····· 1-6
1.3 地址对象 ····· 1-7
1.3.1 概述 ····· 1-7
1.3.2 配置地址对象 ····· 1-8
1.3.3 配置地址组对象 ····· 1-10
1.4 配置服务对象 ····· 1-11
1.4.1 概述 ····· 1-11
1.4.2 预定义服务 ····· 1-11
1.4.3 配置自定义服务 ····· 1-12
1.4.4 配置服务组 ····· 1-13
1.4.5 非标准端口配置 ····· 1-14
1.5 时间对象 ····· 1-15
1.5.1 概述 ····· 1-15
1.5.2 配置日周期计划 ····· 1-15
1.5.3 配置周周期计划 ····· 1-17
1.5.4 配置月周期计划 ····· 1-19
1.5.5 配置单次计划 ····· 1-20
1.5.6 配置单次计划举例 ····· 1-21
1.5.7 配置周周期计划举例 ····· 1-22
1.6 自定义公告 ····· 1-23
1.6.1 概述 ····· 1-23
1.6.2 公告页面 ····· 1-24
1.7 文件类型对象 ····· 1-25

1.7.1 概述 ·····1-25
1.7.2 配置文件类型对象 ·····1-25

1 对象管理

为了方便配置和管理，系统中引入了一些对象的概念，通过这些对象，可以简化配置，提高易用性，本章将介绍以下对象：

- 关键字对象
- URL 对象
- 地址对象
- 服务对象
- 时间对象

在安全控制策略的配置过程中会引用到上面提到的对象。控制策略的配置过程，请参见“控制策略”模块资料。

1.1 关键字对象

1.1.1 关键字对象简介

关键字过滤是多个控制策略功能实现的基础，搜索引擎内容的过滤、HTTP 上传、HTTP 网页内容过滤、邮件控制等都依赖于此。为了简化配置，便于使用，对关键字进行了对象化处理。要使用关键字过滤，首先需要定义相应的关键字对象。定义好的关键字对象可直接在相关功能模块的配置中进行引用。

1.1.2 关键字列表配置

通过菜单“策略配置 > 对象管理 > 关键字对象”，点击<新建>按钮，进入如图 1-1 所示页面。

图1-1 关键字列表

关键字列表的配置项如表 1-1 所示：

表1-1 关键字列表配置项描述表

配置项	说明
名称	关键字列表的名称。
描述	关键字列表的描述。
内容	关键字列表的内容，每行一个。

1.2 URL对象

1.2.1 URL 过滤简介

URL 分类是根据 URL 请求将网站访问分成相应的类别。URL 分类库是进行分类的依据，已经内置在版本当中。用户也可以依据自己的需要，自行定义新的 URL 分类。

通过网站策略对其进行引用，并启用该策略，可以对相关的用户起到网站控制的作用。这样可以通过 HTTP 协议为用户提供应用级的安全防护和访问限制。

注意

- 自定义 URL 分类若与预定义 URL 分类冲突，自定义 URL 的优先级更高。
- 自定义 URL 分类定义以后，即使策略不进行引用，其优先级依然会高于被引用的预定义 URL 分类。

1.2.2 配置 URL 分类

通过菜单“策略配置 > 对象管理> URL 对象 > URL 分类”，进入如图 1-2 所示界面。

图1-2 URL 分类展示界面

URL分类 | 自定义URL | 恶意URL配置 | URL白名单 | HTTPS对象

	名称	描述
1	广告	-
2	成人	-
3	傀儡主机	-
4	艺术	-
5	在线音乐	-
6	机动车	-
7	BBS站点	-
8	键盘记录网站	-
9	博彩	-
10	商业	-
11	计算机与互联网	-
12	犯罪	-
13	钓鱼网站	-
14	毒品	-
15	教育	-
16	娱乐	-
17	在线股票交易	-
18	证券公司	-
19	赌博	-

查看 URL 分类的显示信息如表 1-2 所示：

表1-2 URL 分类显示信息描述表

参数	描述
名称	URL分类名称
描述	URL分类描述

1.2.3 配置自定义 URL

选择菜单“策略配置 > 对象管理> URL 对象 > 自定义 URL”，进入如图 1-3 所示界面。

图1-3 自定义 URL 显示界面

单击“新建”按钮，可以新建自定义 URL，如图 1-4 所示。

图1-4 自定义 URL 配置界面

自定义 URL 的配置信息如表 1-3 所示：

表1-3 自定义 URL 配置描述表

参数	描述
名称	自定义URL的名称，用于外部引用。
内容	自定义URL的匹配内容，每行一条。支持“*”、“/”特殊字符的模糊匹配，以及以http://开头的全URL匹配。

1.2.4 配置恶意 URL

选择菜单“策略配置 > 对象管理> URL 对象 > 恶意 URL 配置”，进入如图 1-5 所示界面。

图1-5 恶意 URL 显示界面

恶意 URL 的配置信息如表 1-4 所示：

表1-4 恶意 URL 配置描述表

参数	描述
恶意URL白名单	恶意URL的白名单，在这里出现的URL不会被当做恶意URL阻断。
恶意URL黑名单	恶意URL的黑名单，在这里出现的URL会被当做恶意URL阻断。

1.2.5 配置 URL 白名单

选择菜单“策略配置 > 对象管理> URL 对象 > URL 白名单”，进入如图 1-6 所示界面。

图1-6 URL 白名单配置界面

恶意 URL 的配置信息如表 1-5 所示：

表1-5 URL 白名单配置描述表

参数	描述
URL白名单	配置URL的白名单，在其它策略中引用。

1.2.6 配置 HTTPS 对象

通过菜单“策略配置 > 对象管理> URL 对象 > HTTPS 对象”，进入如图 1-7 所示。

图1-7 HTTPS 对象界面

单击<新建>按钮，新建 HTTPS 对象，如图 1-8 所示。

图1-8 新建 HTTPS 对象界面

HTTPS 对象配置配置信息如表 1-6 所示：

表1-6 HTTPS 对象配置描述表

参数	描述
名称	HTTPS对象的名称，用作其它策略的引用。
描述	描述信息。
自定义https对象	自定义的https对象折叠框，展开后可自定义对象。
内容	自定义https对象内容。
已选预定分类	已选预定分类，系统默认内建常用对象，可直接引用。
域名列表	选择域名列表。

1.3 地址对象

1.3.1 概述

为了方便用户的配置和管理，设备中引入了地址对象的概念。地址对象分为地址对象和地址组对象。地址组对象是地址对象的集合。在其它功能的配置中，可以引用地址对象来定义配置生效的条件。

1.3.2 配置地址对象

在导航栏中选择“策略配置 > 对象管理 > 地址对象”，点击地址对象标签页，查看所有的地址对象，如图 1-9 所示。点击<新建>按钮，弹出新建地址对象的页面，如图 1-10 所示。

图1-9 地址对象显示页面

		名称	内容(网络，范围，主机，域名)	排除地址	描述	引用	操作
1		any	0.0.0.0/0, ::/0,		任何地址	40	
2		private	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16,		私有地址	5	
3		ChinaUnicom	1.2.2.0/24, 1.4.4.0/24, 1.8.0.0/16, 1.24.0.0/13, 1.45.0.0/16, ...		中国联通	3	
4		ChinaTelecom	1.0.1.0/24, 1.0.2.0/23, 1.0.8.0/21, 1.0.32.0/19, 1.1.0.0/24, ...		中国电信	1	
5		ChinaEducation	1.51.0.0/20, 1.51.16.0/20, 1.51.32.0/19, 1.51.64.0/19, 1.51.96.0/20, ...		中国教育网	1	
6		ChinaMobile	36.128.0.0/12, 36.144.0.0/14, 36.148.0.0/16, 36.149.0.0/16, 36.150.0.0/15, ...		中国移动	2	

图1-10 新建地址对象

地址对象的详细配置表如表 1-7 所示：

表1-7 地址对象的详细配置

配置项		说明
名称		地址对象的名称，为1到31个字符的字符串。
描述		地址对象的描述信息，为0到127个字符的字符串。
地址项目	子网地址	IPv4或IPv6网段地址，例如192.168.1.1/24或2000::1/64。
	范围地址	IPv4或IPv6地址范围，例如192.168.1.1-192.168.1.100或2000:2001:2002:2003::1到2000:2001:2002:2003::5。
	主机地址	IPv4或IPv6主机IP地址，例如192.168.1.1或2000::100。
	域名地址	域名地址，例如www.baidu.com。
已添加项目		已经添加的子网地址、主机地址和范围地址。
排除地址		可排除子网地址、范围地址或主机地址，各项之间以逗号隔开。

点击<提交>按钮，可以完成地址对象的配置。

1.3.3 配置地址组对象

地址组对象是地址对象的集合，设备可以使用地址组对象方便的管理和地址相关的内容。

在导航栏中选择“策略配置 > 对象管理 > 地址对象”，点击“地址组对象”标签页，显示所有的地址组对象，如图 1-11 所示，点击<新建>按钮，弹出地址组对象的配置界面，如图 1-12 所示：

图1-11 地址组对象显示界面

图1-12 新建地址组对象界面

地址组对象的详细配置表 1-8 如示：

表1-8 地址组对象详细配置表

配置项	说明
名称	地址组对象的名称，为1到31个字符的字符串。
描述	地址组对象的描述信息，为0~127个字符的字符串。
选择地址对象	左侧为待选择的地址对象或地址对象组的名称，右侧为已经选择的对象地址。

点击<提交>按钮，完成地址组对象的配置。

1.4 配置服务对象

1.4.1 概述

为了方便用户的配置和管理，设备中引入了服务对象的概念。在其它功能的配置中，可以引用服务对象来定义配置生效的条件。

设备和服务相关的对象有三种：

- 预定义服务，系统预先添加的服务，不可编辑和删除。
- 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。

1.4.2 预定义服务

在导航栏中选择“策略配置 > 对象管理 > 服务对象”，可查看预定义服务，如图 1-13 所示：

图1-13 预定义服务显示界面

预定义服务 | 自定义服务 | 服务组 | 非标准端口配置

	名称	内容(协议:端口开始-端口结束)	引用	描述
1	任何服务		1	任何服务
2	ah	协议:51	0	
3	aol	TCP 目的:5190-5194 源:0-65535	0	
4	bgp	TCP 目的:179-179 源:0-65535	0	
5	bootpc	UDP 目的:68-68 源:0-65535	0	
6	bootps	UDP 目的:67-67 源:0-65535	0	
7	daytime	TCP 目的: 13-13 源:0-65535 UDP 目的: 13-13 源:0-65535	0	
8	dhcp	UDP 目的:67-68 源:0-65535	0	
9	dns	TCP 目的: 53-53 源:0-65535 UDP 目的: 53-53 源:0-65535	0	
10	discard	TCP 目的: 9-9 源:0-65535 UDP 目的: 9-9 源:0-65535	0	
11	esp	协议:50	0	
12	finger	TCP 目的:79-79 源:0-65535	0	
13	ftp	TCP 目的:21-21 源:0-65535	0	
14	gopher	TCP 目的:70-70 源:0-65535	0	
15	gre	协议:47	0	

1.4.3 配置自定义服务

在导航栏中选择“策略配置 > 对象管理 > 服务对象”点击“自定义服务”标签页，进入自定义服务的显示界面，如图 1-14 所示。点击<新建>按钮，弹出新建自定义服务的界面，如图 1-15 所示。

图1-14 自定义服务显示界面

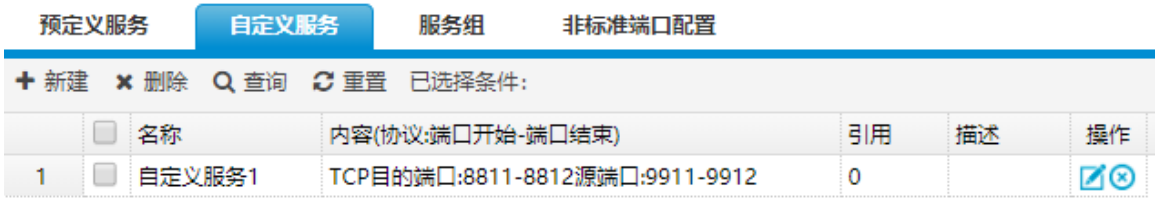


图1-15 添加自定义服务

自定义服务的详细配置如表 1-9 所示：

表1-9 自定义服务详细配置表

配置项	说明
名称	自定义服务的名称，为1到31个字符的字符串。
描述	自定义服务的描述信息，为1到31个字符的字符串。

配置项		说明
添加类型	TCP	TCP的端口范围。
	UDP	UDP的端口范围。
	ICMP	ICMP的code和type。
	协议	IP协议类型。
已添加项目		已经添加的TCP、UDP、ICMP、其它类型。

点击<提交>按钮，完成自定义服务的配置。

1.4.4 配置服务组

在导航栏中选择“策略配置 > 对象管理 > 服务对象”，点击“服务组”标签页，进入显示服务组的页面，如图 1-16 所示。点击<新建>按钮，弹出新建服务组的页面，如图 1-17 所示。

图1-16 服务组显示界面

图1-17 添加自定义服务组

自定义服务组的详细配置如图 1-18 所示。

图1-18 自定义服务组详细配置表

配置项	说明
名称	为新建服务组设置名称。
描述	对新建服务组做描述。
服务子项目	预定义服务、自定义服务或服务组可被添加到服务组中。

点击<提交>按钮，完成自定义服务组的配置。

1.4.5 非标准端口配置

在导航栏中选择“策略配置 > 对象管理 > 服务对象”，点击“非标准端口配置”标签页，进入非标准端口配置的页面，如图 1-19 所示。

图1-19 非标准端口配置界面

非标准端口的详细配置如表 1-10 所示：

表1-10 非标准端口详细配置表

配置项	说明
FTP非标准端口配置	自定义端口列表，最多配置7个，多个端口之间用“,”分开。
TFTP非标准端口配置	添加TFTP自定义端口列表，最多配置7个，多个端口之间用“,”分开。
SIP非标准端口配置	添加SIP自定义端口列表，最多配置7个，多个端口之间用“,”分开。
RTSP非标准端口配置	添加RTSP自定义端口列表，最多配置7个，多个端口之间用“,”分开。

1.5 时间对象

1.5.1 概述

为了方便用户配置和管理，设备中引入了计划任务的概念，计划任务分为周期计划和单次计划。在其它功能的配置中，可以引用计划任务来定义配置生效的条件。

周期时间：包含日计划和周计划，配置服务在指定的周期执行。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。有效时间段之间是或的关系，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。

单次计划：配置服务在指定的单次时间内生效。

1.5.2 配置日周期计划

通过菜单“策略配置 > 对象管理 > 时间对象 > 日计划”，进入如图 1-20 所示页面。在该页面上可以新建、编辑、删除、浏览配置的日周期计划。

图1-20 日周期计划页面

点击<新建>按钮，进入如图 1-21 所示的新建页面，各个配置项的含义如表 1-11 所示。

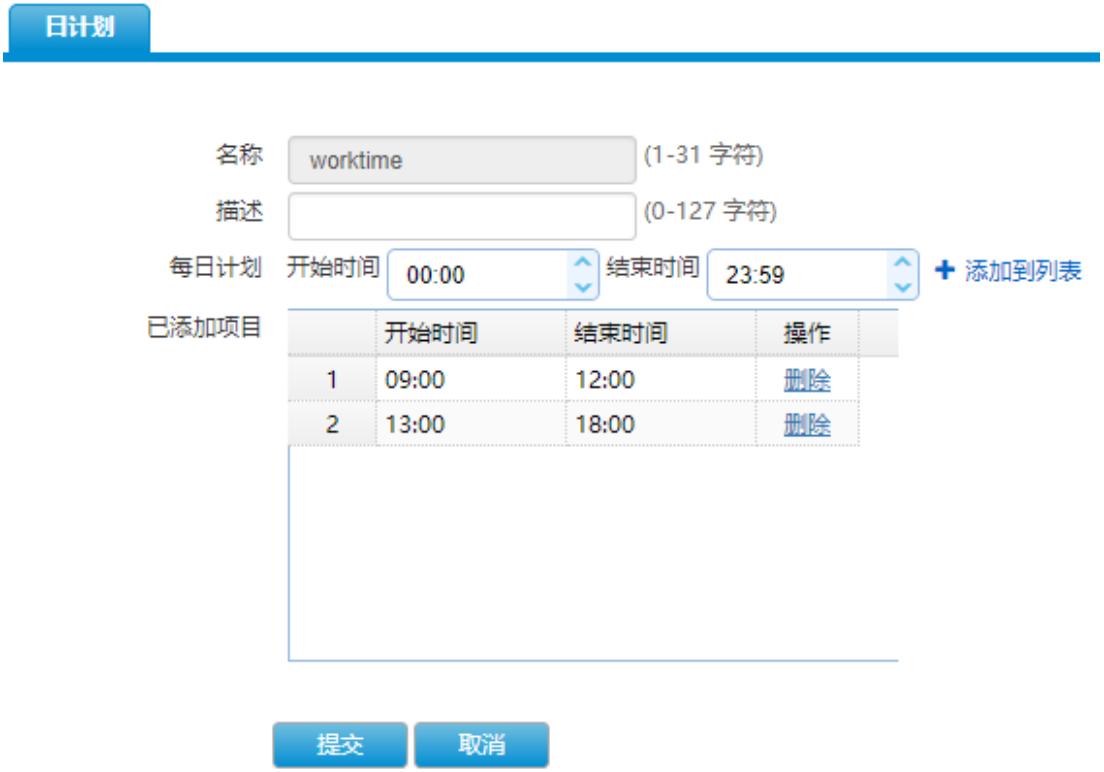
图1-21 添加日计划

表1-11 日计划各个配置项含义描述表

标题项	说明
名称	新建日计划的名称。
描述	新建日计划的简单描述。
开始时间	日计划的起始时间，格式为：小时:分钟。
结束时间	日计划的终止时间，格式为：小时:分钟。
已添加项目	已经添加的开始时间、结束时间。

点击<添加到列表>按钮，将当前的设置添加至日计划。一个日计划，可以添加多个时间计划项目。如图 1-22 所示。

图1-22 添加多个项目至日计划



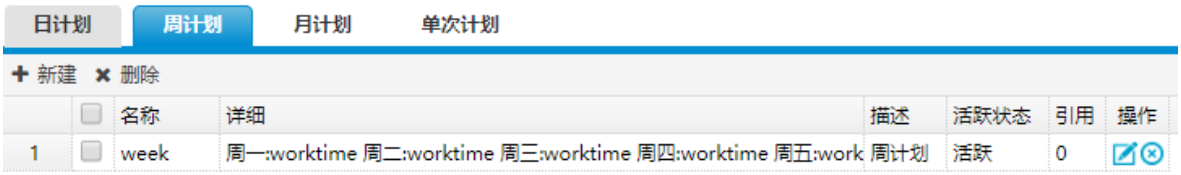
点击<提交>按钮，提交配置。提交配置后，可通过如图 1-23 所示页面查看已配置条目。

图1-23 日计划配置概览页面

1.5.3 配置周周期计划

通过菜单“策略配置 > 对象管理 > 时间对象 > 周计划”，进入如图 1-24 所示页面。在该页面上可以新建、编辑、删除、浏览配置的周周期计划。

图1-24 周周期计划页面



点击<新建>按钮，进入如图 1-25 所示的新建页面，各个配置项的含义如表 1-12 所示。

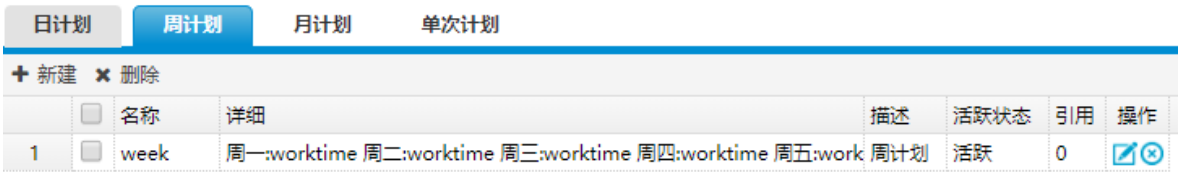
图1-25 添加周计划

表1-12 周计划各个配置项含义描述表

标题项	说明
名称	新建周计划的名称。
描述	新建周计划的简单描述。
周一至周日	为一周的每一天选择对应的日计划。

点击<提交>按钮，提交配置。提交配置后，可通过如图 1-26 所示页面查看已配置条目。

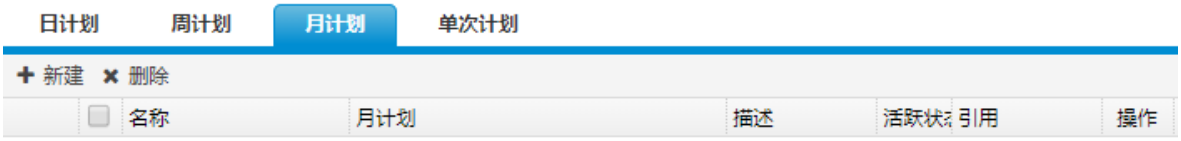
图1-26 周计划配置概览页面



1.5.4 配置月周期计划

通过菜单“策略配置 > 对象管理 > 时间对象 > 月计划”，进入如图 1-27 所示页面。在该页面上可以新建、编辑、删除、浏览配置的月计划。

图1-27 月计划页面



点击<新建>按钮，进入如图 1-28 所示的新建页面，各个配置项的含义如表 1-13 所示。

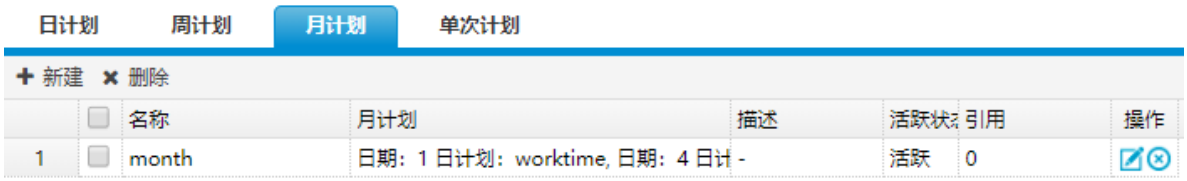
图1-28 添加月计划

表1-13 月计划各个配置项含义描述表

标题项	说明
名称	新建月计划的名称。
描述	新建月计划的简单描述。
开始时间	月计划的开始时间。
结束时间	月计划的结束时间时间。
日计划	为月计划的每一天选择对应的日计划。
已添加项目	已经添加的日期及对应的日计划。

点击<提交>按钮，提交配置。提交配置后，可通过如图 1-29 所示页面查看已配置条目。

图1-29 月计划配置概览页面



1.5.5 配置单次计划

通过菜单“策略配置 > 对象管理 > 时间对象 > 单次计划”，进入如图 1-30 所示页面。在该页面上可以新建、编辑、删除、浏览配置的单次计划。

图1-30 单次计划页面

点击<新建>按钮，进入如图 1-31 所示的新建页面，各个配置项的含义如表 1-14 所示。

图1-31 添加单次计划

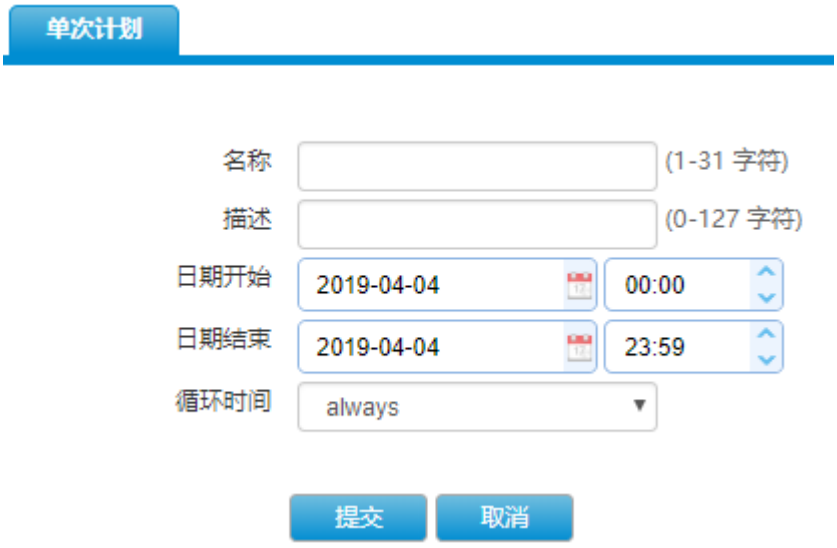
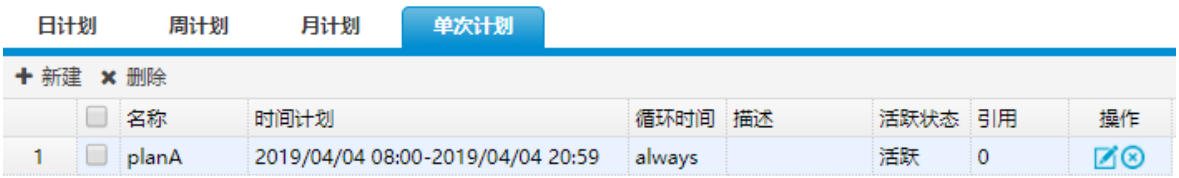


表1-14 单次计划各个配置项含义描述表

标题项	说明
名称	新建单次计划的名称。
描述	新建单次计划的简单描述。
日期开始	有效时间范围的起始时间（年，月，日，时，分）。
日期结束	有效时间范围的终止时间（年，月，日，时，分）。
循环时间	添加从日期开始到日期结束每一天的日计划。

点击<提交>按钮，提交配置。提交配置后，可通过如图 1-32 所示页面查看已配置条目。

图1-32 单次计划配置概览页面



1.5.6 配置单次计划举例

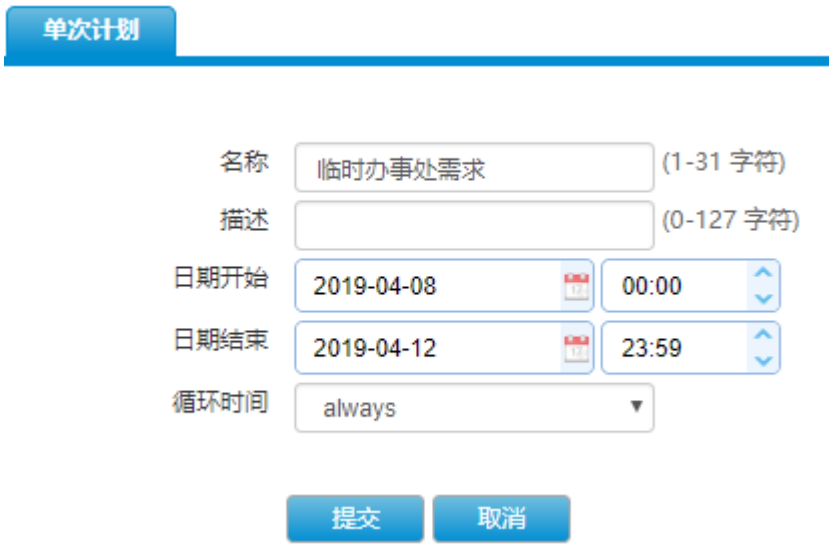
1. 组网需求

增加一个单次计划，此对象目的是为临时办事处创建。为了工作方便设置办事处在有效期间内为外出员工开通 VPN 访问内网资源。

2. 配置步骤

进入单次计划配置页面，按图 1-33 所示进行配置。

图1-33 单次计划配置举例



点击<提交>按钮，提交配置。

3. 验证配置

进入单次计划页面，浏览配置。如图 1-34 所示。

图1-34 单次计划配置举例浏览

1.5.7 配置周周期计划举例

1. 组网需求

配置周周期计划，使不同部门在工作时间内互相访问。

2. 配置步骤

进入周计划配置页面，按图 1-35 所示进行配置。

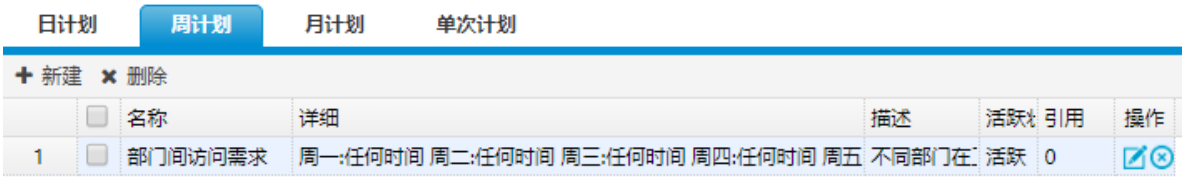
图1-35 周周期计划配置举例

点击<提交>按钮，提交配置。

3. 验证配置

进入周周期计划页面，浏览配置。如图 1-36 所示。

图1-36 周周期计划配置举例浏览



1.6 自定义公告

1.6.1 概述

随着网络化的普及，网络的管理也日趋精细，经常需要在网络内部发布公告或通知内容。网络内部可以选择使用终端公告提醒的公告功能，公告发布后，内网终端能够在访问网页时重定向到公告页面，以达到公告的目的。设备支持推送定制的公告页面，可以用 HTML 或图文编辑方式添加修改公告页面内容。终端公告推送的配置，请参见“控制策略”模块资料。

1.6.2 公告页面

通过菜单“策略配置 > 对象管理 > 公告页面”，进入如图 1-37 所示页面。在该页面上可以配置自定义公告内容。各个配置项含义如表 1-15 所示。

图1-37 公告页面

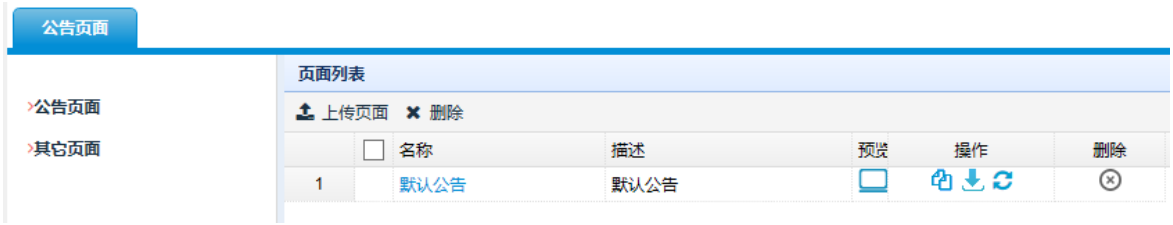
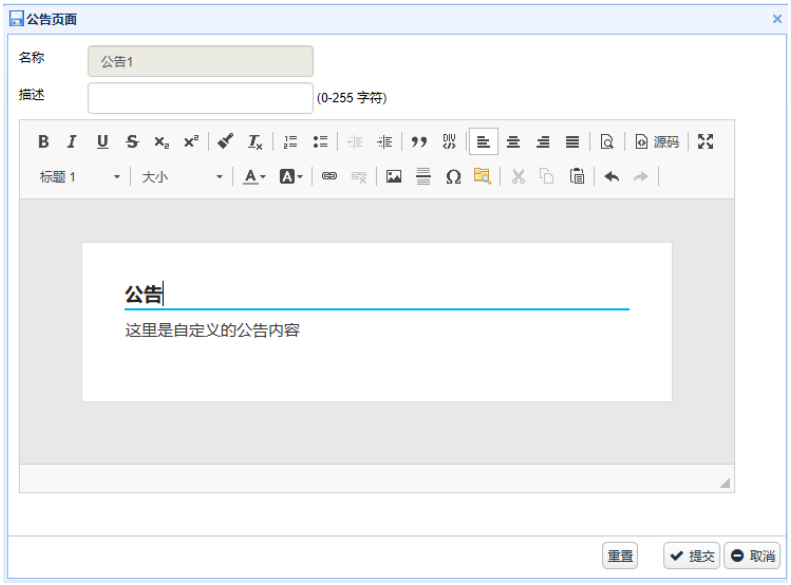


表1-15 自定义公告页面各项含义表

标题项	说明
名称	公告名称，点击进行公告内容编辑。
描述	公告描述信息
预览	公告推送页面预览
操作（复制）	复制公告内容并创建新的公告模板
操作（下载）	导出公告模板
操作（更新）	导入公告并更新现有公告模板
删除	删除公告模板

点击公告名称，可以对公告页面内容进行编辑，如图 1-38 所示。

图1-38 编辑公告页面

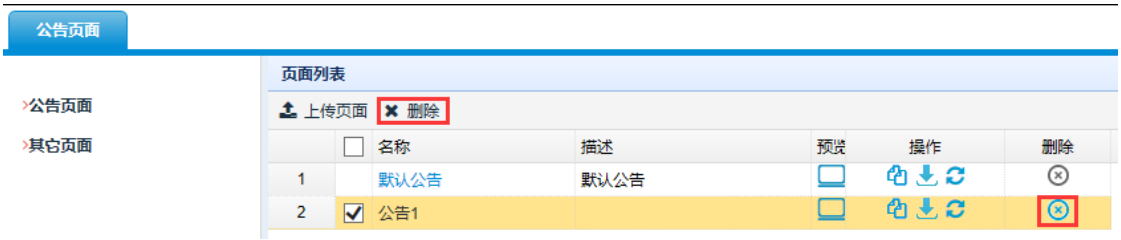


在公告页面，点击<上传页面>按钮，可导入公告并创建一个新的公告模板，如图 1-39 所示

图1-39 公告上传页面

在公告页面，点击<删除>按钮，可删除公告模板，如图 1-40 所示

图1-40 公告删除



1.7 文件类型对象

1.7.1 概述

为了方便用户的配置和管理，设备中引入了文件类型对象的概念。在其它功能的配置中，可以引用文件类型对象来定义配置生效的条件。

在文件类型对象中存在预定义文件类型对象，主要包括：电影、音频、文本、图片、压缩文件、应用程序、office 系列和其它类型文件。

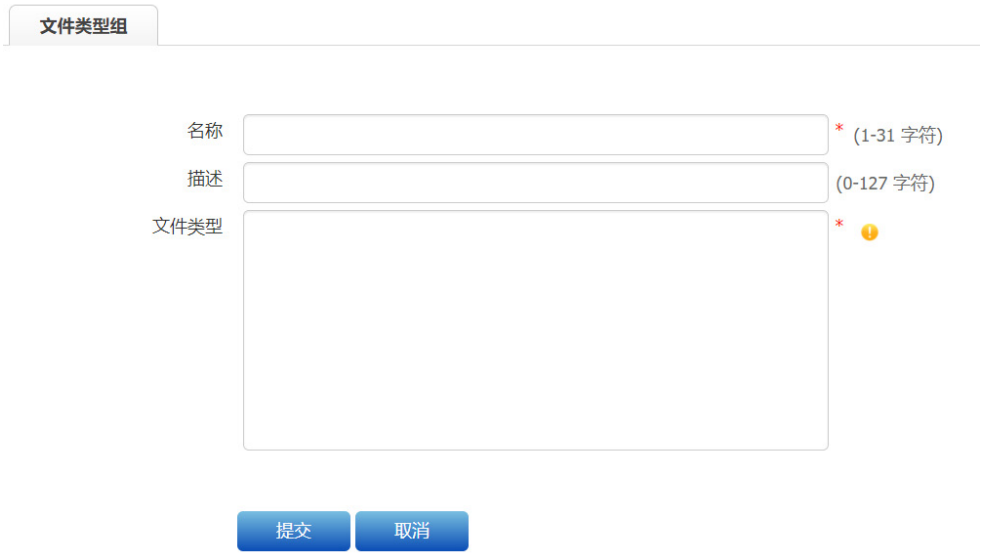
在文件类型对象页面可以修改预定义文件类型对象，也可以新增自定义文件类型对象。

1.7.2 配置文件类型对象

在导航栏中选择“策略配置 > 对象管理 > 文件类型对象”，进入文件类型对象标签页，查看所有的文件类型对象，如图 1-41 所示。点击<新建>按钮，弹出新建文件类型对象的页面，如图 1-42 所示。

图1-41 文件类型对象显示页面

图1-42 新建文件类型对象



文件类型对象的详细配置表如表 1-16 所示：

表1-16 文件类型对象的详细配置

配置项	说明
名称	文件类型对象的名称，为1到31个字符的字符串。
描述	文件类型对象的描述信息，为0到127个字符的字符串。
文件类型	可以配置具体文件类型对象，多个文件类型用换行输入，每条允许输入1-15个字符，最多支持64个，格式：*.mp3或.mp3或mp3。

点击<提交>按钮，可以完成文件类型对象的配置。

目 录

1 应用对象 ····· 1-1
1.1 应用对象简介 ····· 1-1
1.2 应用对象 ····· 1-1
1.3 应用标签对象 ····· 1-2
1.4 自定义应用 ····· 1-4
1.4.1 自定义应用简介 ····· 1-4
1.4.2 自定义应用页面 ····· 1-4
1.4.3 自定义应用设置规则 ····· 1-5
1.5 应用智能识别 ····· 1-7
1.5.1 应用智能识别简介 ····· 1-7
1.5.2 应用智能识别页面 ····· 1-7
1.5.3 应用智能识别-P2P 行为 ····· 1-8
1.5.4 应用智能识别-迅雷 ····· 1-9
1.6 应用识别模式配置 ····· 1-10
1.7 配置应用识别高级配置 ····· 1-11
1.8 配置举例 ····· 1-12
1.8.1 应用对象配置举例 ····· 1-12
1.8.2 应用对象标签配置举例 ····· 1-13
1.8.3 自定义应用配置举例 ····· 1-15
1.8.4 应用智能识别配置举例 ····· 1-17

1 应用对象

1.1 应用对象简介

为了方便用户配置和管理，设备中引入了应用对象的概念。应用对象分为应用对象和应用标签对象两大类，在其它功能模块（如控制策略、IPv6 策略、流量控制策略模块）可以引用应用对象来配置匹配条件以及子策略等。

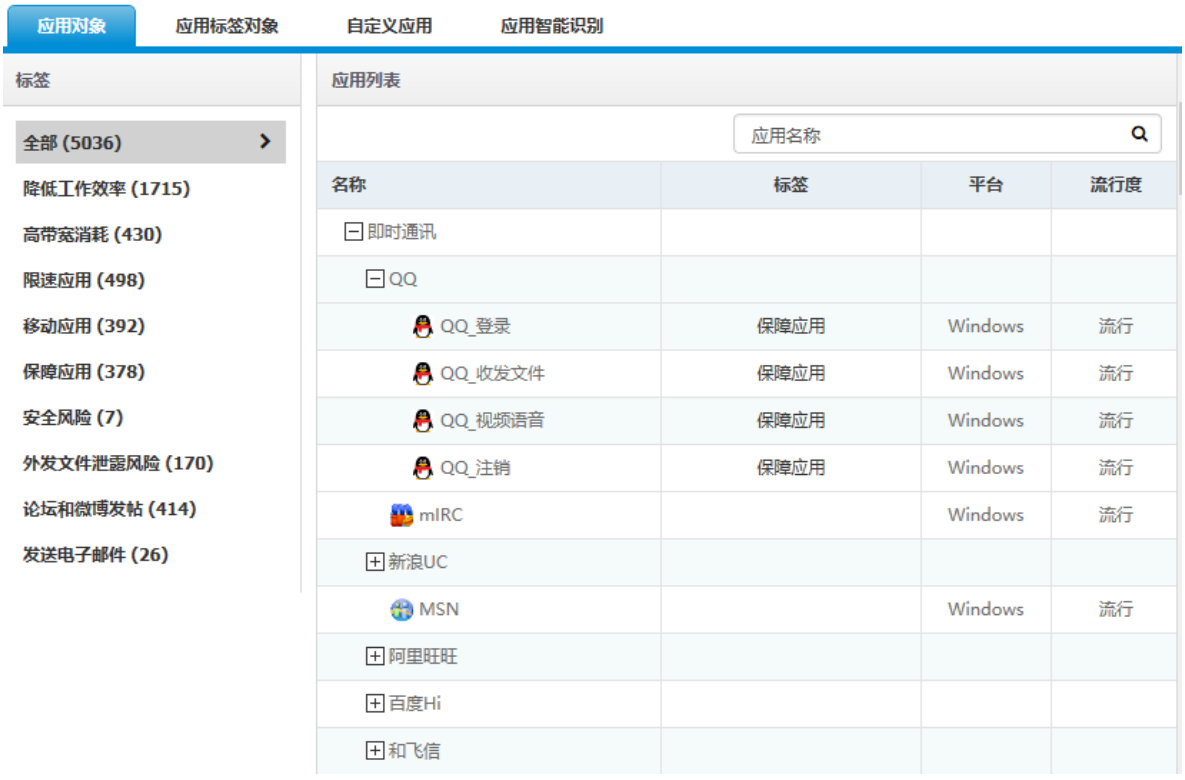
应用对象基于特征进行分析并通过应用组、应用、应用行为三级目录树结构展示，应用对象和应用标签对象在控制策略、IPv6 控制策略、流量控制等模块都是以树形结构展示，可以方便的进行查询及引用。

控制策略的配置过程，请参见“控制策略”、“IPv6 控制策略”及“流控策略”模块资料。

1.2 应用对象

在导航栏中选择“策略配置 > 对象管理 > 应用对象”，进入应用对象显示页面，可以查看设备上支持的所有应用对象，如图 1-1 所示。

图1-1 应用对象显示页面



应用对象页面各项参数含义如表 1-1 所示。

表1-1 应用对象页面各项参数含义表

配置项	说明
标签	应用及应用行为对应的标签类，系统内置9个预定义标签。
应用列表	展示详细的应用及应用行为列表，显示该应用或应用行为所属标签以及对应的系统平台，还有应用的流行度展示。
查询	根据应用名称进行查询。

1.3 应用标签对象

在导航栏中选择“策略配置 > 对象管理 > 应用对象”，点击“应用标签对象”标签页，如图 1-2 所示。

图1-2 应用标签对象显示界面

应用标签对象页面详细参数如表 1-2 所示。

表1-2 应用标签对象页面详细参数表

配置项	说明
名称	应用标签对象的名称。
描述	新建应用标签对象添加的描述信息。
内容（应用对象）	选择的应用对象。
操作	操作包括编辑和删除两项： 编辑：可对描述和内容进行修改编辑操作； 删除：对选中对象进行删除操作。

点击<新建>按钮，可以新建一条应用标签对象，如图 1-3 所示。

图1-3 新建应用标签对象

点击<提交>按钮，完成自定义应用标签对象的配置，如图 1-4 所示。

图1-4 应用标签对象自定义配置完成

自定义配置好的应用标签对象可以在应用对象页面上展示，如图 1-5 所示。

图1-5 应用对象组展示自定义应用标签对象

1.4 自定义应用

1.4.1 自定义应用简介

通用的应用无法满足客户的需求，客户需要根据自己定义的规则，标识为自定义的应用。从而方便管理和监控整个网络。

1.4.2 自定义应用页面

在导航栏中选择“策略配置 > 对象管理 > 应用对象”，点击“自定义应用”标签页，进入自定义应用页面，如图 1-6 所示。

图1-6 自定义应用设置页面

表1-3 自定义应用页面详细说明

项目	说明
新建	新建一个自定义应用
删除	删除一个自定义应用
全部删除	全部删除自定义应用
导入	导入自定义应用
导出	导出自定义应用
启用	启用自定义应用
禁用	禁用自定义应用

1.4.3 自定义应用设置规则

在导航栏中选择“策略配置 > 对象管理 > 应用对象 > 自定义应用>”点击<新建>，进入自定义应用配置规则页面，如图 1-7 所示。

图1-7 自定义应用设置规则页面

页面的详细说明如表 1-4 所示。

表1-4 自定义应用配置详细说明

项目	说明
启用	该自定义应用是否开启匹配。
名称	应用名称

项目	说明
描述	自定义应用的描述信息。
风险级别	应用的风险级别，分为低、中、高三个级别。
应用类	选择应用的应用类别，比如QQ就是即时通讯。
数据包方向	数据包方向，包含任意、请求数据和响应数据。 • 任意：包含请求数据和响应数据。 • 请求数据：只匹配请求的数据。 • 响应数据：只匹配响应的数据。
协议	自定义应用的协议类型：any、TCP、UDP、OTHER，默认值any，表示匹配系统支持的所有应用协议类型。
端口	自定义应用规则要匹配的端口，多个配置以回车分割，最多支持5个端口配置。
IP地址	输入自定义应用规则要匹配的IP地址。
目标域名	输入自定义应用规则要匹配的域名，支持模糊匹配。
匹配模式	应用匹配模式，包含文本和正则表达式。 • 文本：应用以文本的方式匹配。 • 正则表达式：应用以正则表达式方式匹配。
DNS域名学习模式	DNS域名的学习模式，包含引用数据包特征中的目标域名和指定域名。 • 引用数据包特征中的目标域名：引用的是上述目标域名。 • 目标域名：自定义域名，支持模糊匹配，多个匹配以回车分割，最多支持 64 个域名配置。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

1.5 应用智能识别

1.5.1 应用智能识别简介

当前迅雷可通过多种方式（如：FTP、HTTP、P2P 下载等）下载资源，单独限制迅雷下载，效果不佳，应用智能识别功能可有效的提高迅雷下载流量识别率。

当前部分 P2P 软件无法通过应用特征识别，应用智能识别功能可通过 P2P 行为来智能识别 P2P 流量。

1.5.2 应用智能识别页面

在导航栏中选择“策略配置>对象管理>应用对象>应用智能识别”，进入应用智能识别页面，如图 1-8 所示。

图1-8 应用智能识别页面

页面的详细说明如表 1-5 所示

表1-5 应用智能识别页面详细说明

项目	说明
状态	启用/禁用功能状态展示，默认功能开启。
应用名称	应用智能识别名称。
应用类型	应用智能识别归属应用分类。
应用描述	应用智能识别描述。
检测宽松度	应用智能识别的宽松度级别展示。

1.5.3 应用智能识别-P2P 行为

在导航栏中选择“策略配置>对象管理>应用对象>应用智能识别”，点击“P2P 行为”右边的<编辑>按钮，进入 P2P 行为配置页面，如图 1-7 所示。

图1-9 P2P 行为配置页面

页面的详细说明如表 1-4 所示。

表1-6 P2P 行为详细说明

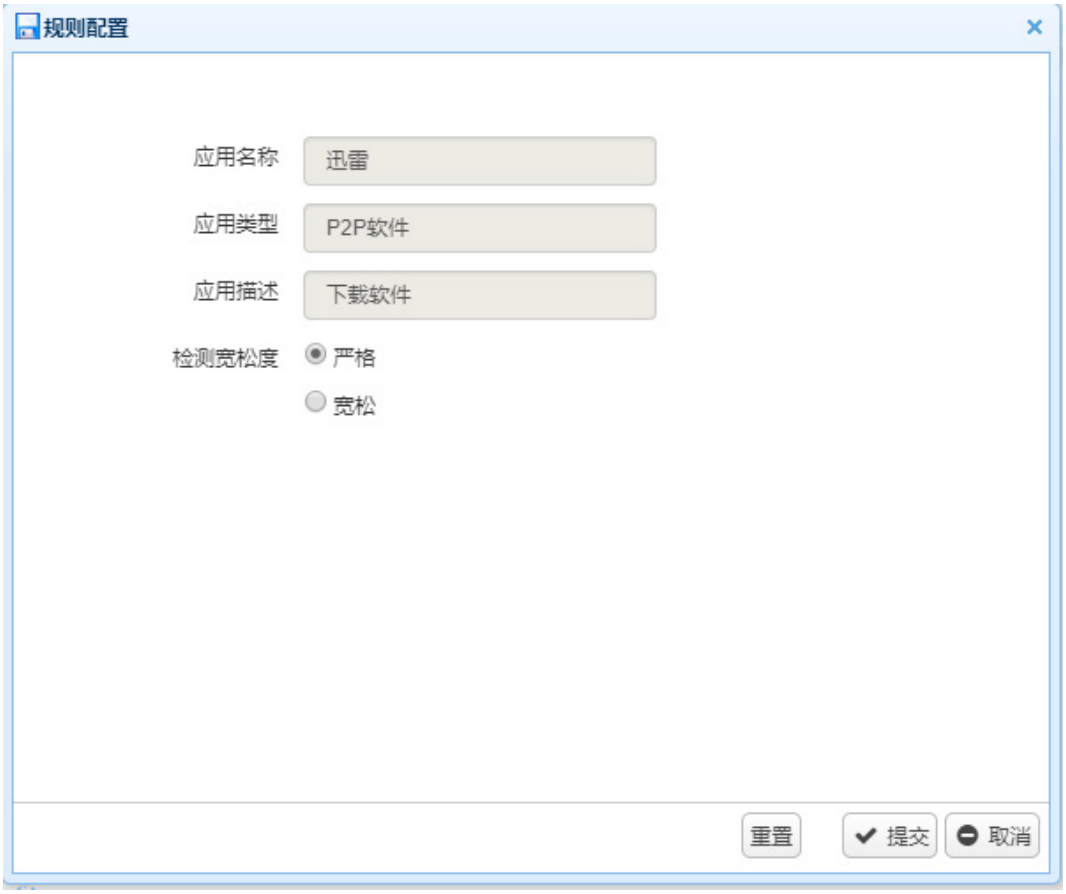
项目	说明
启用	启用/禁用P2P行为识别功能。
应用名称	应用智能识别名称。
应用类型	应用智能识别归属应用分类。
应用描述	应用智能识别描述。
检测宽松度	单选框，有3个级别：严格、适中、宽松。 • 严格：识别要求严格，可能存在漏报； • 适中：识别要求适中，默认配置； • 宽松：识别要求宽松，可能存在误报。
排除扫描端口	排除P2P智能识别端口。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

1.5.4 应用智能识别-迅雷

在导航栏中选择“策略配置>对象管理>应用对象>应用智能识别”，点击“迅雷”右边的<编辑>按钮，进入迅雷配置页面，如图 1-10 所示。

图1-10 迅雷配置页面



页面的详细说明如表 1-7 所示。

表1-7 迅雷配置详细说明

项目	说明
应用名称	应用智能识别名称。
应用类型	应用智能识别归属应用分类。
应用描述	应用智能识别描述。
检测宽松度	单选框，有2个级别：严格、宽松。 • 严格：识别要求严格，默认配置； • 宽松：识别要求宽松，可能存在误报。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

1.6 应用识别模式配置

通过菜单“策略配置 > 对象管理 > 应用识别模式”，进入应用识别模式配置显示页面，如图 1-11 所示。

图1-11 应用识别模式配置页面

页面的详细说明如表 1-8 所示。

表1-8 应用识别模式配置描述表

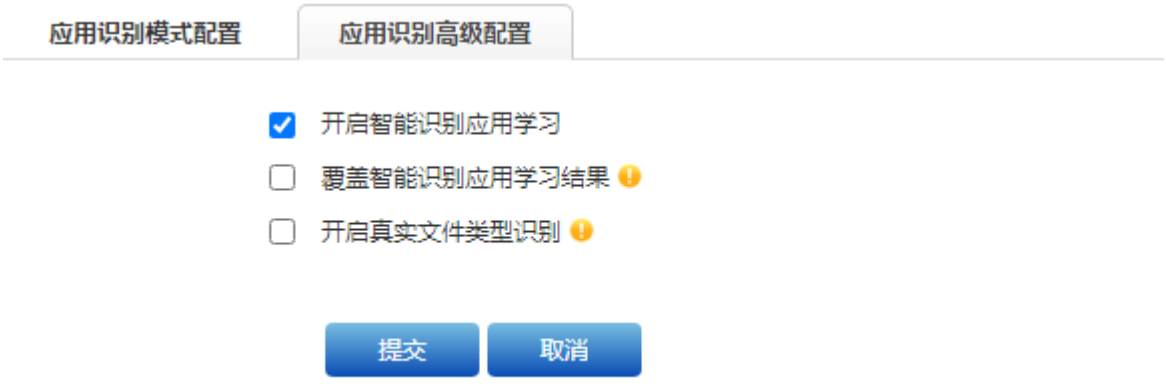
项目	说明
智能模式	应用引擎模式将尽可能的尝试用各种方式识别网络流量
快速模式	应用引擎模式将关闭部分智能分析功能以提高性能
关闭模式	应用引擎模式将不进行应用识别

选择完毕后，点击<提交>按钮，应用配置。

1.7 配置应用识别高级配置

通过菜单“策略配置 > 对象管理 > 应用识别模式>应用识别高级配置”，进入应用识别高级配置显示页面，如图 1-12 所示。

图1-12 应用识别模式配置页面



页面的详细说明如表 1-9 所示。

表1-9 应用识别高级配置描述表

项目	说明
开启智能识别应用学习	智能识别学习应用结果。
覆盖智能识别应用学习结果	用户访问不同网站，智能识别应用学习结果可能相同。启用此选项学习结果覆盖，智能识别应用为最新学习结果。
开启真实文件类型识别	通过特征识别文件，配置文件类型过滤功能使用。

选择完毕后，点击<提交>按钮，应用配置。

1.8 配置举例

1.8.1 应用对象配置举例

1. 组网需求

某企业内网用户访问外网时，工作时间禁止登录即时通讯软件。

2. 配置步骤

进入“策略配置 > 控制策略”，新建一条控制策略，行为选择允许，基础条件使用默认配置，在应用过滤中新建一条应用控制策略，配置应用对象选择“即时通讯”类的应用组如图 1-13 所示，动作配置拒绝，日志级别选择通知级别，如图 1-14 所示；高级配置中时间选择工作时间，点击策略下的<提交>按钮，控制策略配置完成，如图 1-15 所示。

图1-13 应用控制策略应用对象选择即时通讯类配置

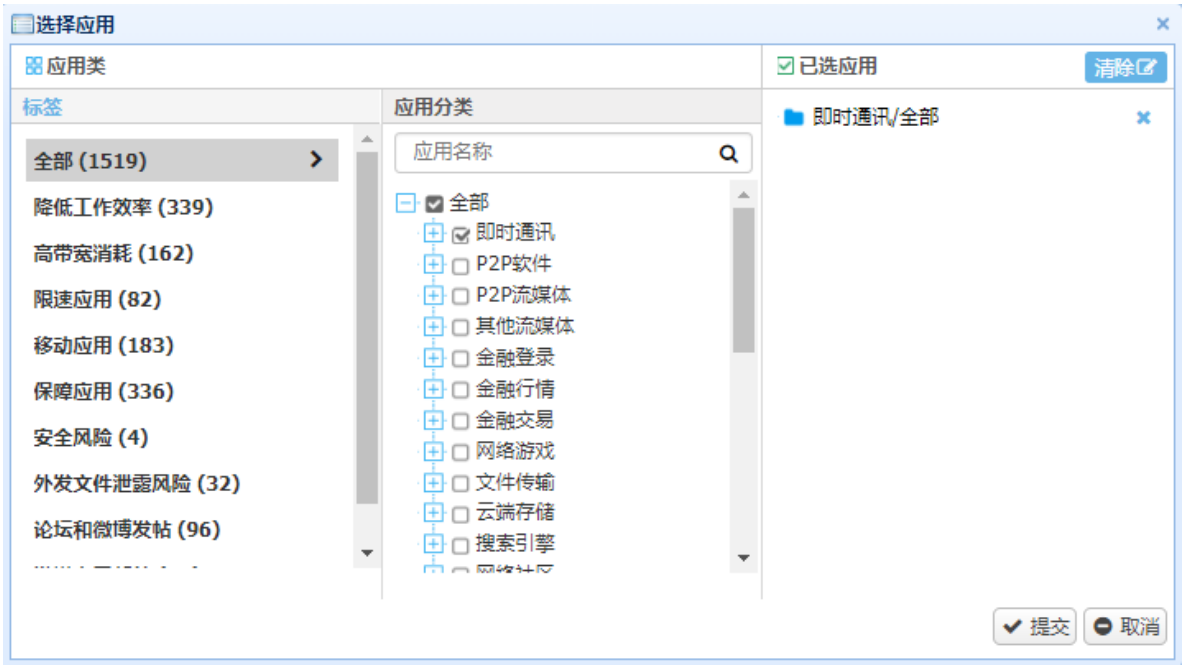


图1-14 应用控制策略配置完成

图1-15 控制策略配置完成

3. 验证配置

测试终端过设备登录即时通讯软件，无法登录成功，且在“数据中心>日志中心>控制日志>应用控制日志”页面上有相应的阻断日志记录，如图 1-16 所示。

图1-16 应用控制日志

1.8.2 应用对象标签配置举例

1. 组网需求

某企业内网用户访问外网时，工作时间禁止在论坛微博上发帖。

2. 配置步骤

进入“策略配置>控制策略”，新建一条控制策略，行为选择拒绝，勾选日志，匹配条件应用中选择应用标签“论坛和微博发贴”类标签如图 1-17 所示，高级配置中时间选择工作时间，点击<提交>按钮，控制策略配置完成，如图 1-18 所示。

图1-17 应用选择应用标签对象配置

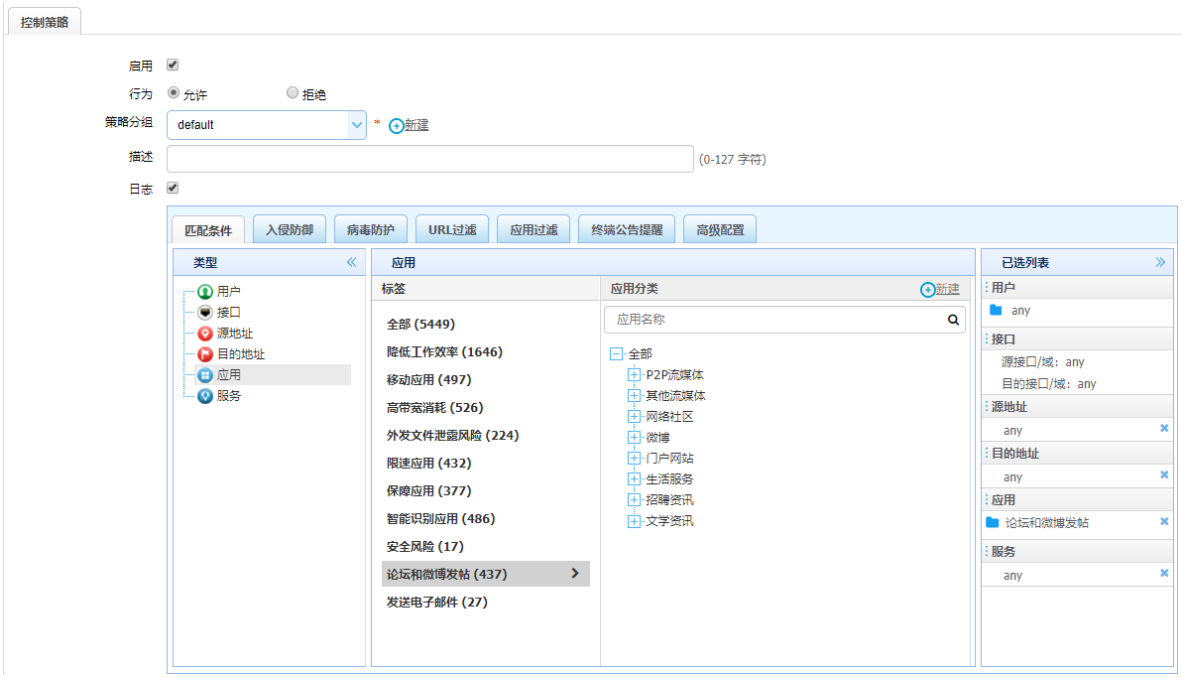


图1-18 控制策略配置完成

3. 验证配置

测试终端过设备访问外网论坛微博网站进行发表评论说说时，发表失败如图 1-19 所示。

图1-19 微博发表失败

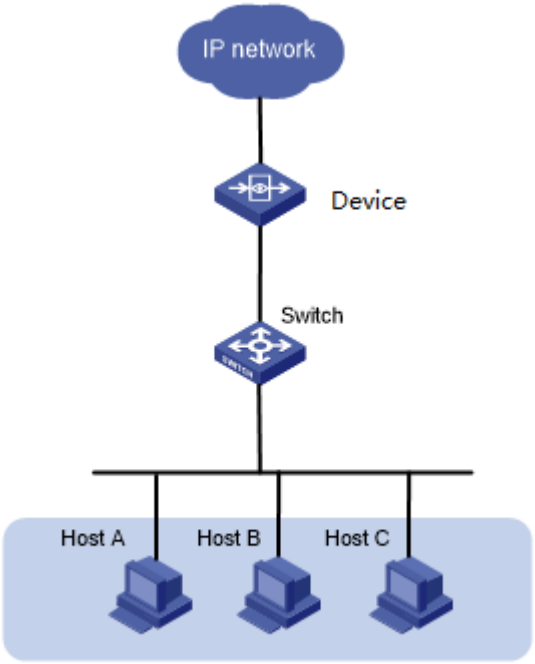
1.8.3 自定义应用配置举例

1. 组网需求

用户匹配自定义规则流量过设备，会话监控查看识别到自定义应用。

2. 组网图

图1-20 组网图



3. 配置步骤

(1) 新建自定义应用，名称设置为“AAA”，协议选择 UDP，应用类选择“流媒体”，目标端口填写“65”。

图1-21 配置自定义应用

(2) HOST 匹配自定义应用流量过设备，会话监控页面显示被识别。

图1-22 会话监控页面显示被识别

	用户	用户组	源地址	源端口	目的地址	目的端口	协议	类型	应用	发送流量	接收流量	总流量	创建时间
1	192.168.200.172	匿名用户组	192.168.200.172	65	220.10.1.2	8080	UDP	半连接	AAA	860(B)	0(B)	860(B)	2019-03-29 16:40:04
2	192.168.200.182	匿名用户组	192.168.200.182	65	220.10.1.2	8080	UDP	半连接	AAA	860(B)	0(B)	860(B)	2019-03-29 16:40:39
3	192.168.1.61	匿名用户组	192.168.200.37	65	220.10.1.2	8080	UDP	半连接	AAA	1.62(MB)	0(B)	1.62(MB)	2019-03-29 04:30:02

1.8.4 应用智能识别配置举例

1. 组网需求

禁止公司员工进行迅雷下载。

2. 配置步骤

(1) 配置应用智能识别

进入“策略配置>对象管理>应用对象>应用智能识别”，点击“迅雷”右边的<编辑>按钮，进入迅雷配置页面，系统默认智能识别功能已开启，如图 1-23 所示。

图1-23 应用智能识别配置

(2) 在导航栏中选择“策略配置 > 控制策略”，单击<新建>按钮，进入控制策略配置页面，点击<应用过滤>页签，进入应用过滤配置页面，新建一条迅雷下载应用阻断策略，如图 1-24 所示。

图1-24 控制策略配置

点击<提交>按钮，提交配置。

3. 验证配置

配置完成后，公司员工无下载迅雷资源，且在设备上有记录阻断日志，如图 1-25 所示。

图1-25 应用控制阻断日志

应用控制日志

查询 重置 导出 **查询结果:** 在 2019-04-04 约 33 条日志记录中，从 1 - 33 搜索出相关结果 33 条

	用户	用户mac	应用分类	应用	策略类型	处理动作	终端类型	级别	时间	操作
1	192.168.8.99	1c:1b:0d:03:ca:d4	P2P软件	迅雷_下载	应用控制	阻断	未知类型	警告	2019-04-04 15:21:22	详细
2	192.168.8.99	1c:1b:0d:03:ca:d4	P2P软件	迅雷_下载	应用控制	阻断	未知类型	警告	2019-04-04 15:21:13	详细
3	192.168.8.99	1c:1b:0d:03:ca:d4	P2P软件	迅雷_下载	应用控制	阻断	未知类型	警告	2019-04-04 15:20:58	详细
4	192.168.8.99	1c:1b:0d:03:ca:d4	P2P软件	迅雷_下载	应用控制	阻断	未知类型	警告	2019-04-04 15:20:48	详细
5	192.168.8.99	1c:1b:0d:03:ca:d4	P2P软件	迅雷_下载	应用控制	阻断	未知类型	警告	2019-04-04 15:20:33	详细
6	192.168.8.99	1c:1b:0d:03:ca:d4	P2P软件	迅雷_下载	应用控制	阻断	未知类型	警告	2019-04-04 15:20:23	详细
7	192.168.8.99	1c:1b:0d:03:ca:d4	P2P软件	迅雷_下载	应用控制	阻断	未知类型	警告	2019-04-04 15:20:08	详细
8	192.168.8.99	1c:1b:0d:03:ca:d4	P2P软件	迅雷_下载	应用控制	阻断	未知类型	警告	2019-04-04 15:20:03	详细
9	192.168.8.99	1c:1b:0d:03:ca:d4	P2P软件	迅雷_下载	应用控制	阻断	未知类型	警告	2019-04-04 15:19:58	详细
10	192.168.8.99	1c:1b:0d:03:ca:d4	P2P软件	迅雷_下载	应用控制	阻断	未知类型	警告	2019-04-04 15:19:53	详细

目 录

1 CA 服务器 ····· 1-1
1.1 CA 简介 ····· 1-1
1.2 根证书管理 ····· 1-1
1.3 CRL 管理 ····· 1-4
1.4 用户证书管理 ····· 1-5
1.5 典型配置举例 ····· 1-10
1.5.1 配置 CA 根证书 ····· 1-10
1.5.2 配置用户证书 ····· 1-11

1 CA 服务器

1.1 CA简介

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。

本功能具有如下功能点：

- 作为可信任机构，管理维护根证书，发布证书撤销列表(CRL)。
- 作为可信任机构，签发用户证书，撤销用户证书。
- 通过 TFTP 协议，配合 TFTP 服务器，设备可对存在的用户证书进行管理和维护。

1.2 根证书管理

通过菜单“策略配置 > 对象管理 > CA 服务器 > 根 CA 配置管理 > 根证书管理”，进入如图 1-1 所示的页面。在该页面上，可以生成、导入、导出 CA 根证书。

图1-1 根证书管理页面

点击<生成 CA 根证书>按钮，进入如图 1-2 所示页面，生成 CA 根证书，各个配置项的含义如表 1-1 所示。

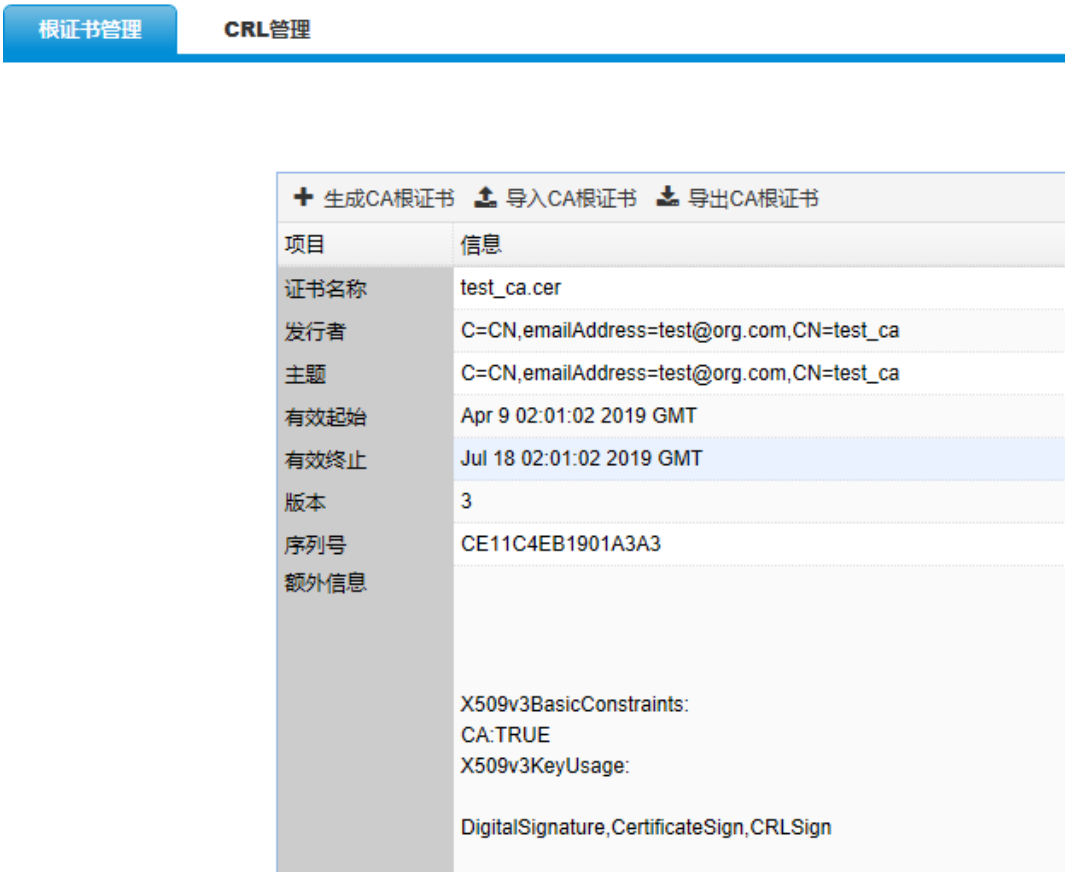
图1-2 CA 根证书配置页面

表1-1 CA 根证书配置项含义描述表

标题项	说明
证书名称	根CA证书的名称。
部门	CA证书的部门信息。
组织	CA证书的所属组织。
位置(城市)	CA证书所在的位置。
州/省	CA证书所属的州或省。
国家/地区	CA证书的国家或地区信息。
电子邮件	CA证书持有者的联系方式。
有效期	CA证书的有效时间。
密码	CA证书的保护密码。
密钥大小	CA证书对应私钥的大小。

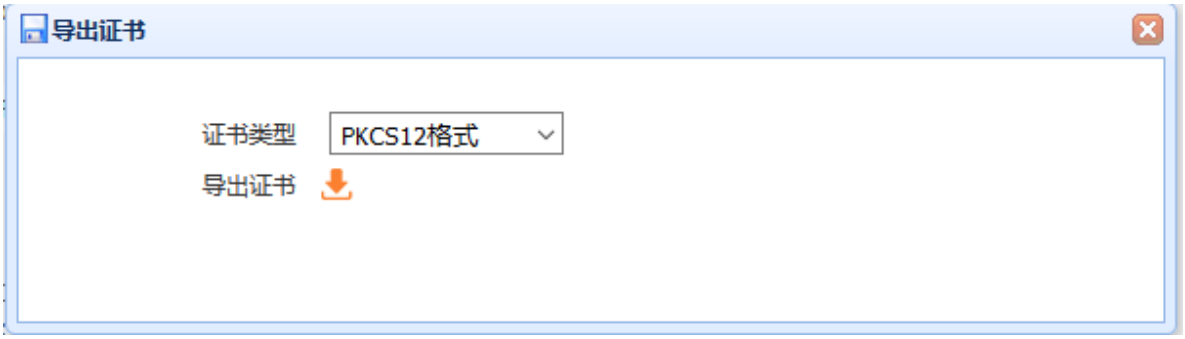
点击<提交>按钮，提交配置，生成 CA 根证书，如图 1-3 所示。

图1-3 CA 根证书页面



点击<导出 CA 根证书>，可以通过 TFTP 协议，导出 CA 根证书至 TFTP 服务器。导出页面如图 1-4 所示。

图1-4 导出 CA 根证书页面



可选择导出为 PKCS12 格式的单个证书，或者证书密钥分离格式的证书。

点击<导入 CA 根证书>，可以通过 TFTP 协议，从 TFTP 服务器导入 CA 根证书。导入页面如图 1-5 所示。各个配置项含义如表 1-2 所示。

图1-5 导入 CA 根证书页面

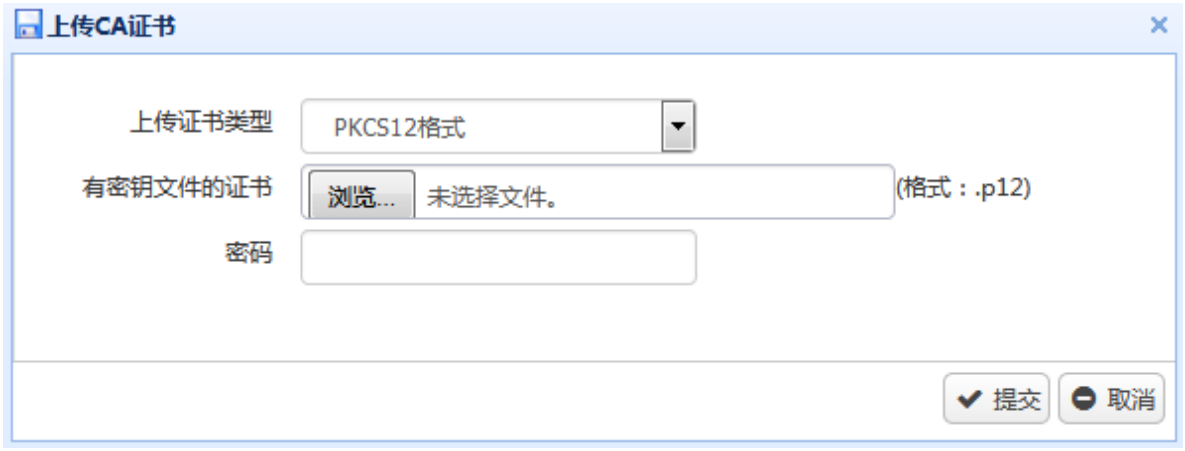


表1-2 导入 CA 根证书配置项含义描述表

标题项	说明
上传证书类型	上传证书的类型，可以上传如下类型： • 单个证书：PKCS12 格式的证书，证书和密钥文件一体。 • 证书密钥分离：PEM 格式的证书，证书文件和密钥文件分离。
证书文件	证书密钥分离格式的证书文件。
密钥文件	证书密钥分离格式的密钥文件。
有密钥文件的证书	单个证书格式的证书文件。
密码	单个证书格式证书的保护密码。

1.3 CRL管理

通过菜单“策略配置 > 对象管理 > CA 服务器 > 根 CA 配置管理 > CRL 管理”，进入如图 1-6 所示的页面。在该页面上，可以更新、导出、配置 CRL 自动更新周期。各个配置项含义如表 1-3 所示。

图1-6 CRL 管理页面

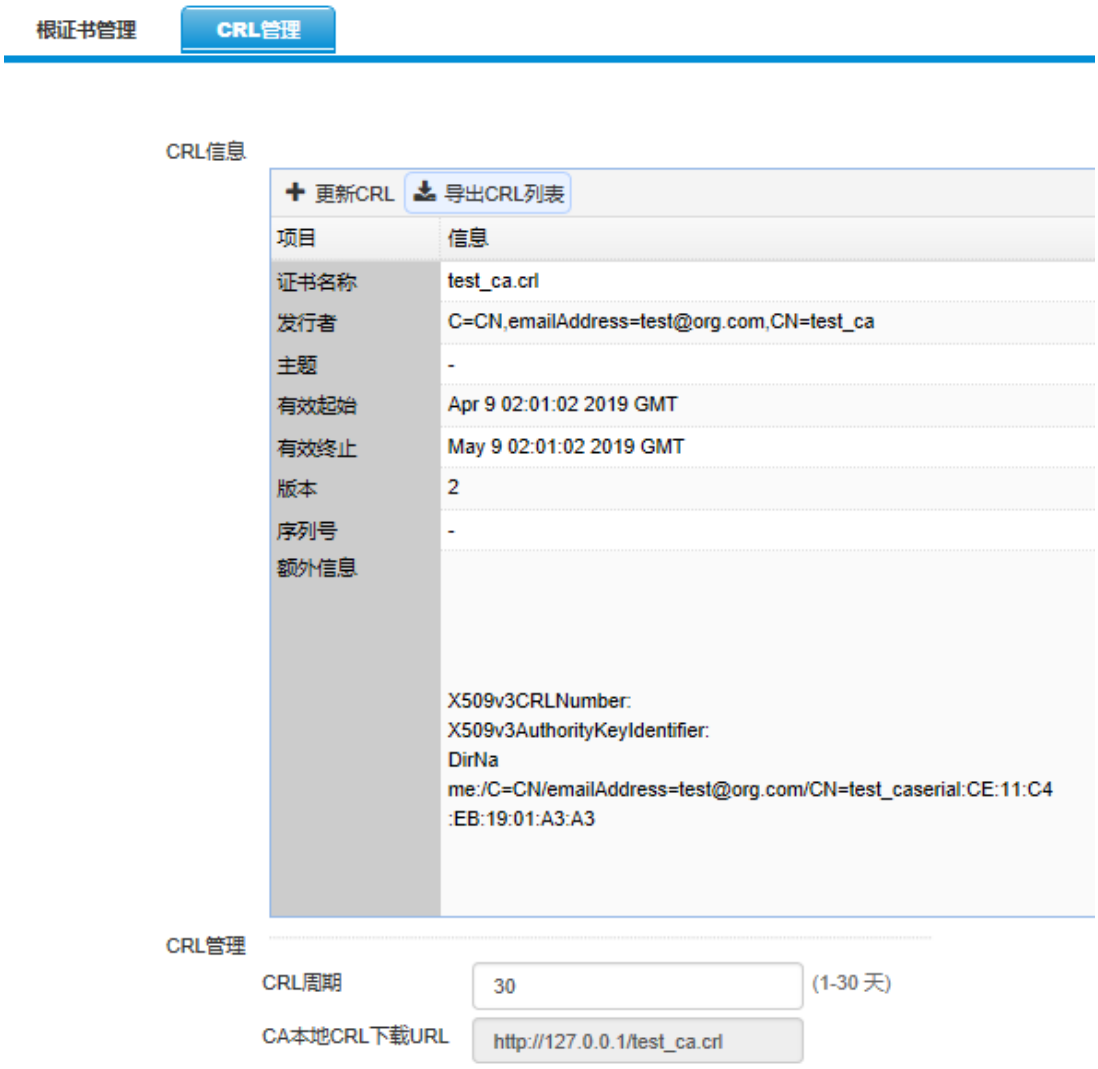


表1-3 CRL 配置项含义描述表

标题项	说明
CRL周期	CRL文件自动更新的周期
CA本地CRL下载URL	通过HTTP协议下载CRL文件的URL

点击<更新 CRL>按钮，可以立刻更新 CRL 文件。

点击<导出 CRL 列表>，可以通过 TFTP 协议，导出 CRL 文件至 TFTP 服务器。

1.4 用户证书管理

通过菜单“策略配置 > 对象管理 > CA 服务器 > 用户证书管理”，进入如图 1-7 所示的页面。在该页面上，可以生成、签发、撤销、删除、导出用户证书。

图1-7 用户证书管理页面

点击<生成证书请求>按钮，进入如图 1-8 所示的页面，各个配置项的含义如表 1-4 所示。

图1-8 用户证书请求生成页面

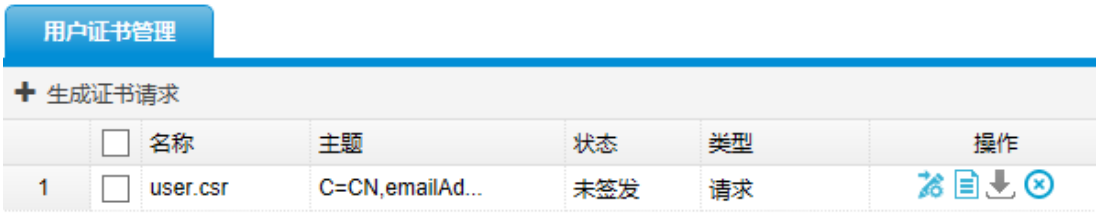
表1-4 用户证书请求各个配置项含义表

标题项	说明
证书名称	用户证书的名称。
部门	用户证书的部门信息。
组织	用户证书的所属组织。
位置(城市)	用户证书所在的位置。
州/省	用户证书所属的州或省。

标题项	说明
国家/地区	用户证书的国家或地区信息。
电子邮件	用户证书持有者的联系方式。
密钥大小	用户证书对应私钥的大小。

点击<提交>按钮，提交配置。提交配置后可通过如图 1-9 所示的页面查看。

图1-9 用户证书概览页面



点击<签发>按钮，进入如图 1-10 所示的页面签发用户证书。各个配置项含义如表 1-5 所示。

图1-10 用户证书请求签发页面

表1-5 用户证书请求签发配置项含义描述表

标题项	说明
有效期	签发的用户证书的有效期
密码	用户证书的保护密码

点击<提交>按钮，提交配置。提交完配置后的页面如图 1-11 所示。在签发完证书后，就可以进行撤销、复制、查看、导出、删除的操作。

图1-11 用户证书请求签发后页面

点击<复制>按钮，可以将选中的证书复制到本地用户证书中。

点击<删除>按钮，可以删除选中的证书。

点击<撤销>按钮，可以撤销选中的证书。撤销页面如图 1-12 所示。各个配置项含义如表 1-6 所示。

图1-12 用户证书撤销页面

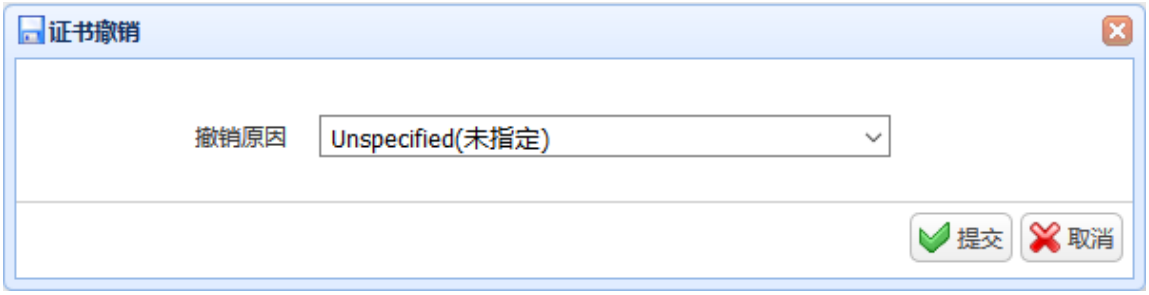
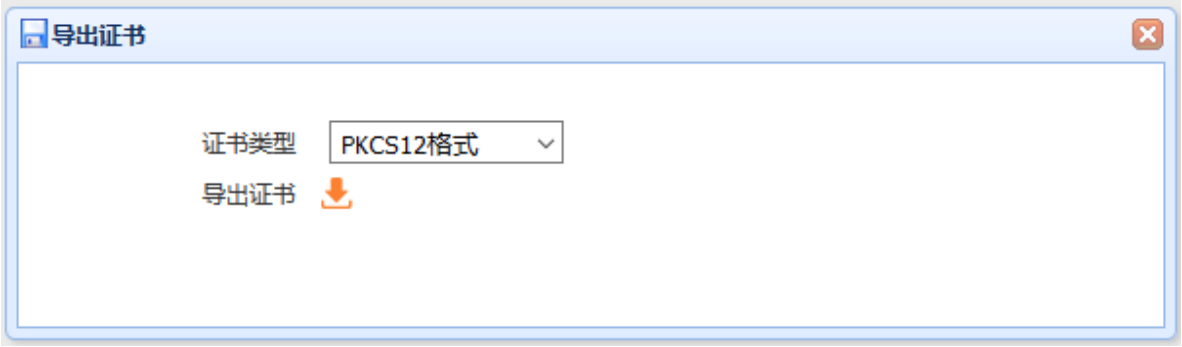


表1-6 用户证书撤销配置项含义描述表

标题项	说明
撤销原因	撤销用户证书的原因，有如下原因： • Unspecified：未指定撤销原因 • KeyCompromise：私钥泄露 • CaCompromise：CA 泄露 • Affiliation Changed：从属关系改变

点击<导出>按钮，可以通过 TFTP 协议，导出用户证书至 TFTP 服务器。导出页面如图 1-13 所示。

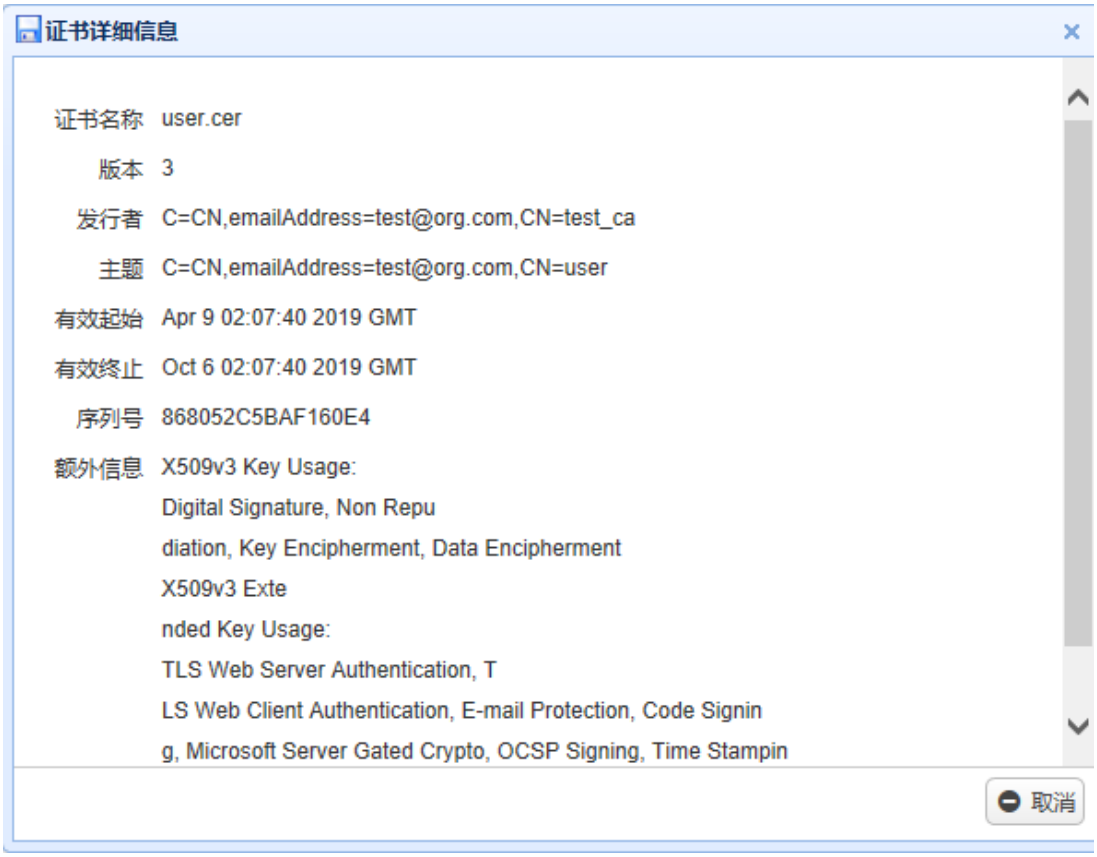
图1-13 导出用户证书页面



可选择导出为 PKCS12 格式的单个证书，或者证书密钥分离格式的证书。

点击<详细信息>按钮，可以查看用户证书的详细信息。如图 1-14 所示。

图1-14 用户证书的详细信息



1.5 典型配置举例

1.5.1 配置 CA 根证书

1. 组网需求

创建 CA 根证书。

2. 配置步骤

进入根证书管理页面。按图 1-15 所示配置。

图1-15 配置 CA 根证书

点击<提交>按钮，提交配置。

3. 验证配置

进入根证书管理页面，查看 CA 根证书，如图 1-16 所示。

图1-16 CA 根证书

1.5.2 配置用户证书

1. 组网需求

创建用户证书请求，并签发用户证书。

2. 配置步骤

(1) 进入用户证书管理页面，生成用户证书请求，如图 1-17 所示。

图1-17 生成用户证书请求

点击<提交>按钮，提交配置。

(2) 点击<签发>按钮，签发用户证书。如图 1-18 所示。

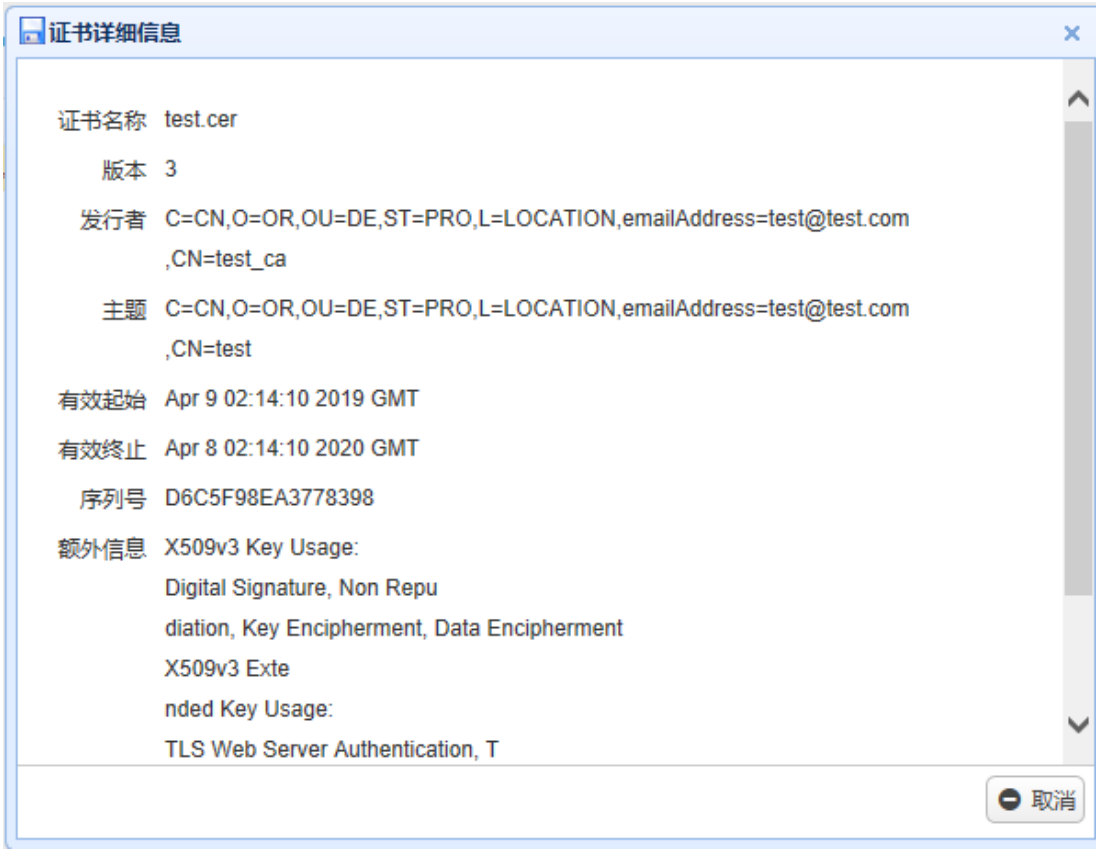
图1-18 签发用户证书请求

点击<提交>按钮，提交配置。

3. 验证配置

进入用户证书管理页面，查看用户证书，如图 1-19 所示。

图1-19 用户证书


证书详细信息
证书名称 test.cer
版本 3
发行者 C=CN,O=OR,OU=DE,ST=PRO,L=LOCATION,emailAddress=test@test.com
,CN=test_ca
主题 C=CN,O=OR,OU=DE,ST=PRO,L=LOCATION,emailAddress=test@test.com
,CN=test
有效起始 Apr 9 02:14:10 2019 GMT
有效终止 Apr 8 02:14:10 2020 GMT
序列号 D6C5F98EA3778398
额外信息 X509v3 Key Usage:
Digital Signature, Non Repu
diation, Key Encipherment, Data Encipherment
X509v3 Exte
nded Key Usage:
TLS Web Server Authentication, T
取消

目 录

1 本地证书 ····· 1-1
1.1 本地证书简介 ····· 1-1
1.2 本地用户证书 ····· 1-1
1.3 本地 CA 证书 ····· 1-3
1.4 本地 CRL ····· 1-5
1.5 国密证书 ····· 1-7
1.6 自动获取 CRL ····· 1-9
1.7 典型配置举例 ····· 1-10
1.7.1 用户证书配置举例 ····· 1-10
1.7.2 自动获取 CRL 配置举例 ····· 1-11

1 本地证书

1.1 本地证书简介

本地证书包含本地用户证书，本地 CA 证书，CRL，以及 CRL 自动更新。本地用户证书是用于设备某些模块，如 IPsec，在建立连接时，向远端设备进行身份验证；本地 CA 证书是用于设备在与远端设备建立连接时，对远端设备进行身份验证；CRL 为远端设备的身份验证提供验证条件。

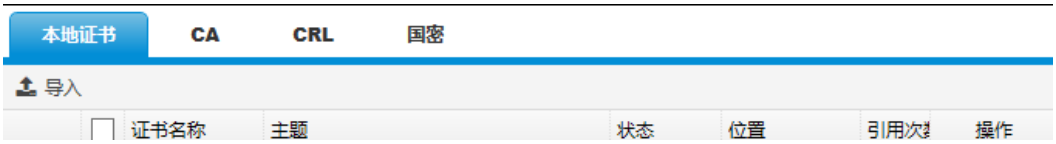
本功能具有如下功能点：

- 本地用户证书的管理和维护。
- 本地 CA 证书的管理和维护。
- 本地 CRL 的管理和维护。包括通过 TFTP Server 进行 CRL 文件的管理和维护，以及自动获取 CRL 文件的配置管理。

1.2 本地用户证书

通过菜单“策略配置 > 对象管理 > 本地证书 > 证书 > 本地证书”，进入如图 1-1 所示页面。在该页面上，可以导入、导出、删除、查看本地用户证书。

图1-1 本地用户证书页面



点击<导入>按钮，导入本地用户证书，如图 1-2 所示。各个配置项的含义如表 1-1 所示。

图1-2 导入本地用户证书

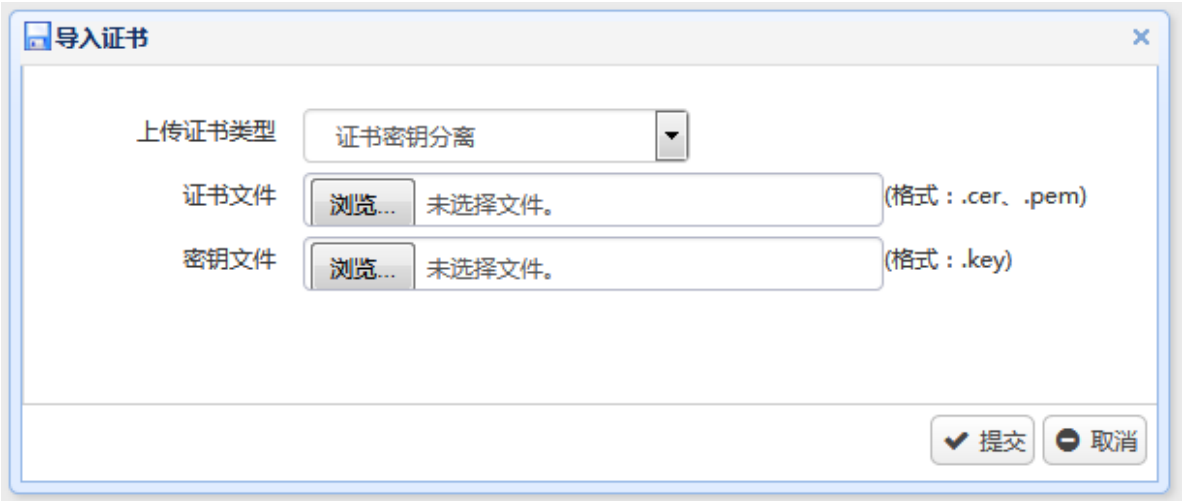
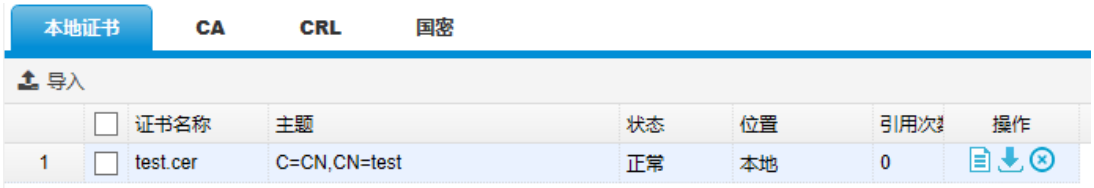


表1-1 导入证书各个配置项含义描述表

标题项	说明
上传证书类型	上传证书的类型，可以上传如下类型： • 单个证书：PKCS12 格式的证书，证书和密钥文件一体。 • 证书密钥分离：PEM 格式的证书，证书文件和密钥文件分离。
证书文件	证书密钥分离格式的证书文件。
密钥文件	证书密钥分离格式的密钥文件。
有密钥文件的证书	单个证书格式的证书文件。
密码	单个证书格式证书的保护密码。

点击<提交>按钮，提交配置后，可以通过如图 1-3 所示的本地用户证书页面导出、查看、删除导入的用户证书。

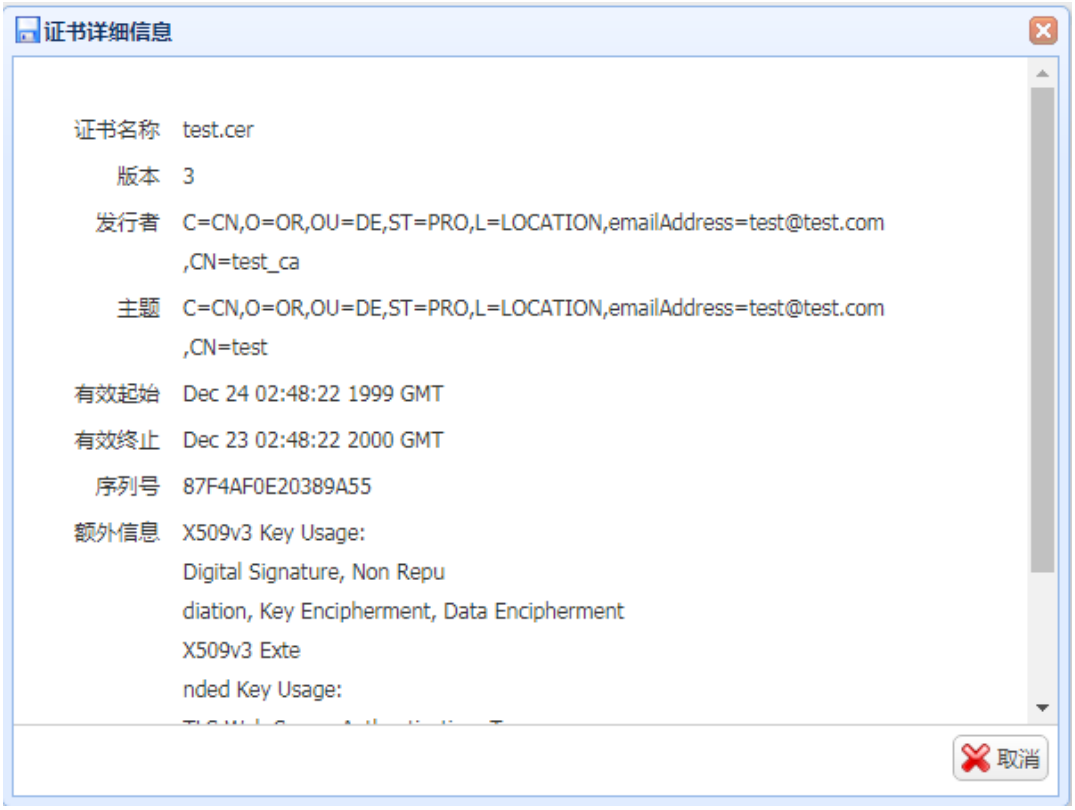
图1-3 本地用户证书概览页面



点击<删除>按钮，可以删除选中的条目。

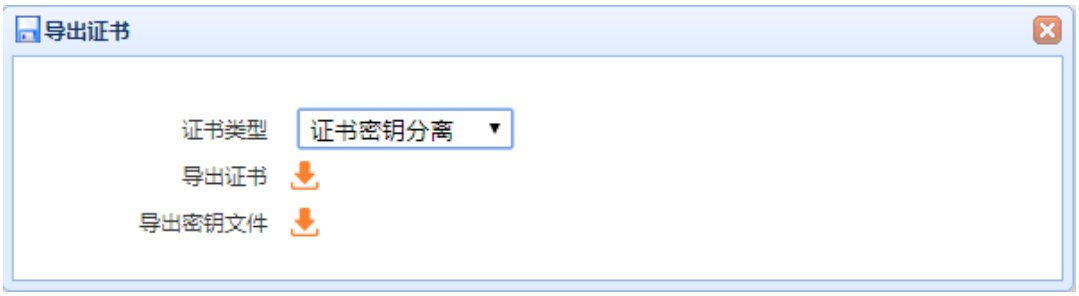
点击<详细信息>按钮，可以查看证书的详细信息。如图 1-4 所示。

图1-4 查看本地用户证书的详细信息



点击<导出>按钮，可以导出本地用户证书。如图 1-5 所示。

图1-5 导出本地用户证书页面

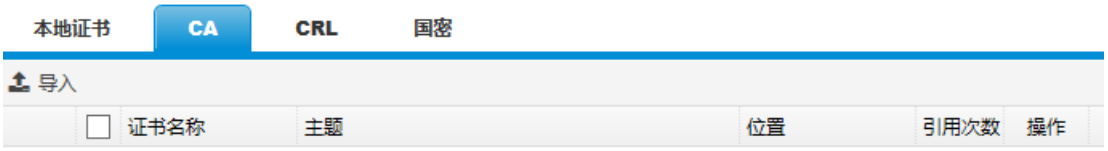


可以选择导出 PKCS12 格式的单个证书文件，或者 PEM 格式的证书密钥分离文件。

1.3 本地CA证书

通过菜单“策略配置 > 对象管理 > 本地证书 > 证书 > CA”，进入如图 1-6 所示页面。在该页面上，可以导入、导出、删除、查看本地 CA 证书。

图1-6 本地 CA 证书页面



点击<导入>按钮，导入本地 CA 证书，如图 1-7 所示。各个配置项的含义如表 1-2 所示。

图1-7 导入本地 CA 证书

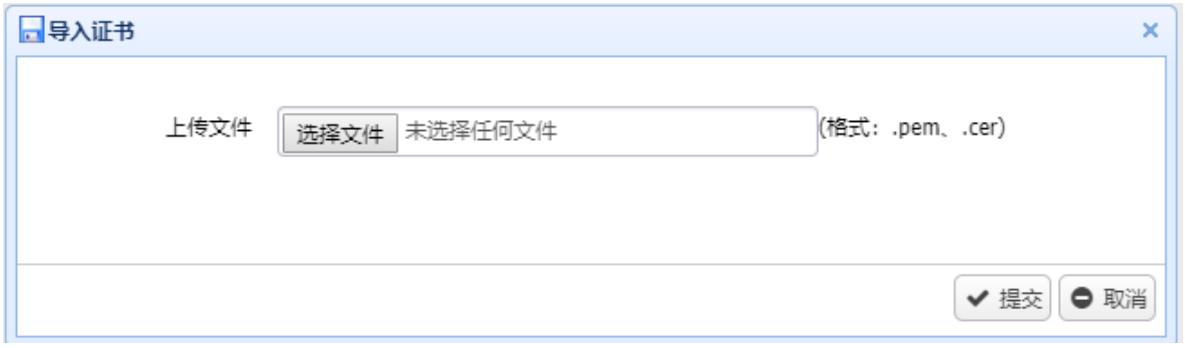
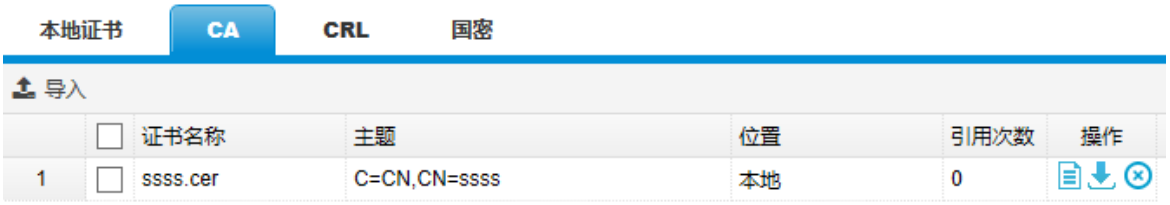


表1-2 导入证书各个配置项含义描述表

标题项	说明
上传文件	上传的CA证书文件，支持.cer、.pem格式的证书文件。

点击<提交>按钮，提交配置后，可以通过如图 1-8 所示的本地 CA 证书页面导出、查看、删除导入的 CA 证书。

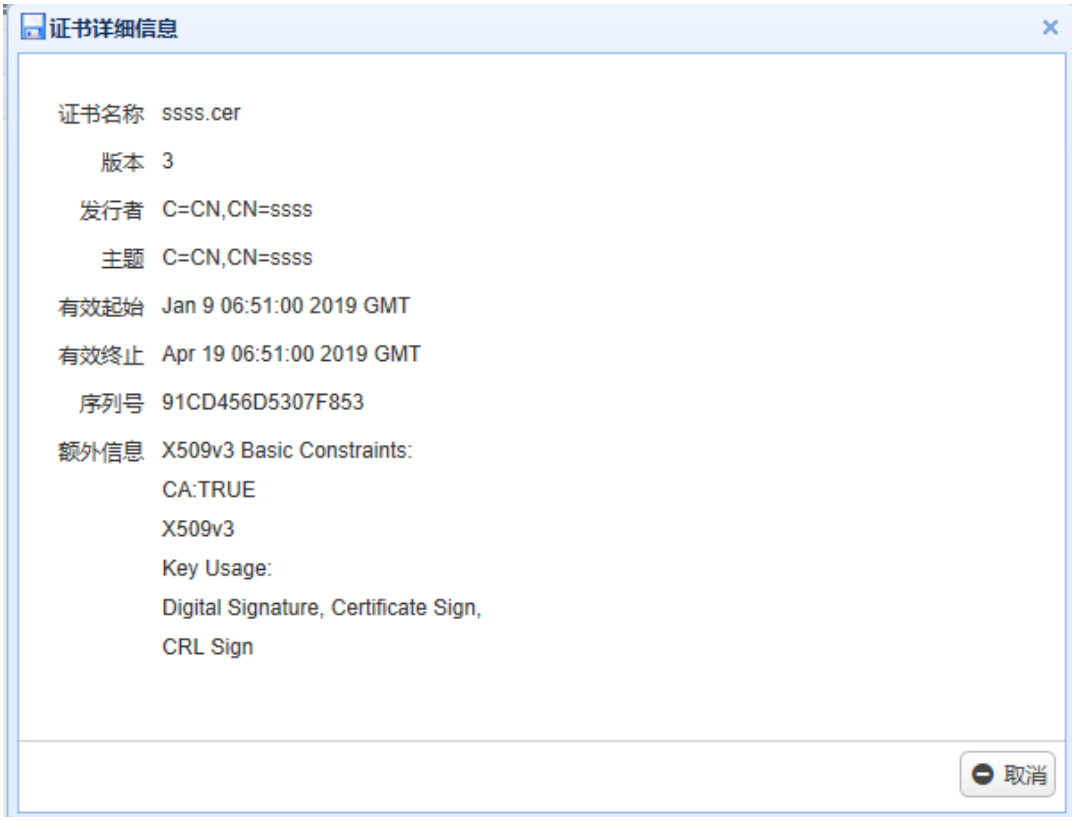
图1-8 本地 CA 证书概览页面



点击<删除>按钮，可以删除选中的条目。

点击<详细信息>按钮，可以查看证书的详细信息。如图 1-9 所示。

图1-9 查看本地 CA 证书的详细信息

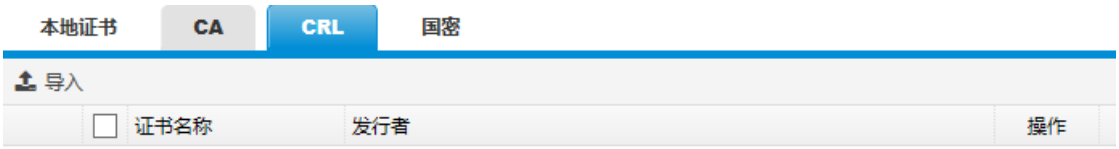


点击<导出>按钮，可以导出本地 CA 证书。

1.4 本地CRL

通过菜单“策略配置 > 对象管理 > 本地证书 > 证书 > CRL”，进入如图 1-10 所示页面。在该页面上，可以导入、导出、删除、查看本地 CRL 文件。

图1-10 本地 CRL 文件页面



点击<导入>按钮，导入 CRL 文件，如图 1-11 所示。各个配置项的含义如表 1-3 所示。

图1-11 导入 CRL 文件

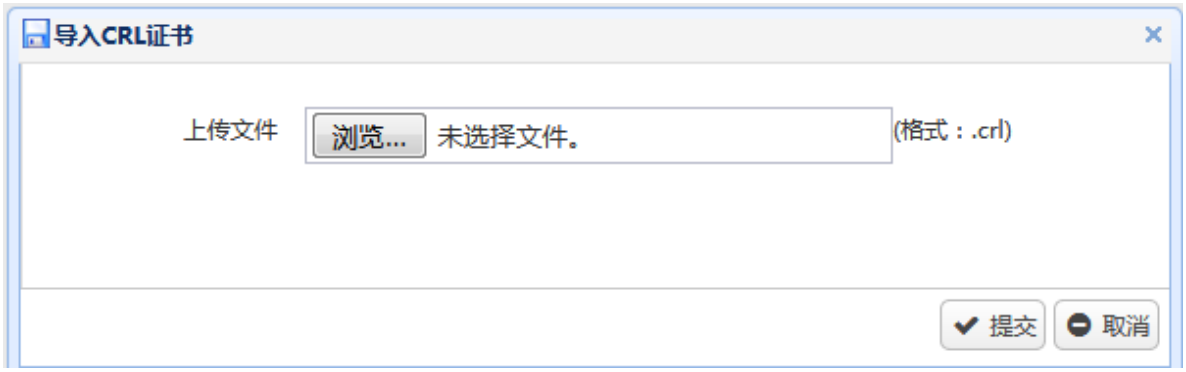
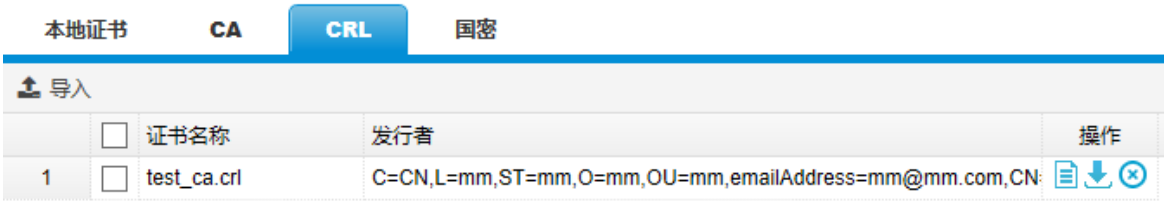


表1-3 导入 CRL 各个配置项含义描述表

标题项	说明
上传文件	上传的CRL文件，支持.crl格式的文件。

点击<提交>按钮，提交配置后，可以通过如图 1-12 所示的本地 CRL 页面导出、查看、删除导入的 CRL 文件。

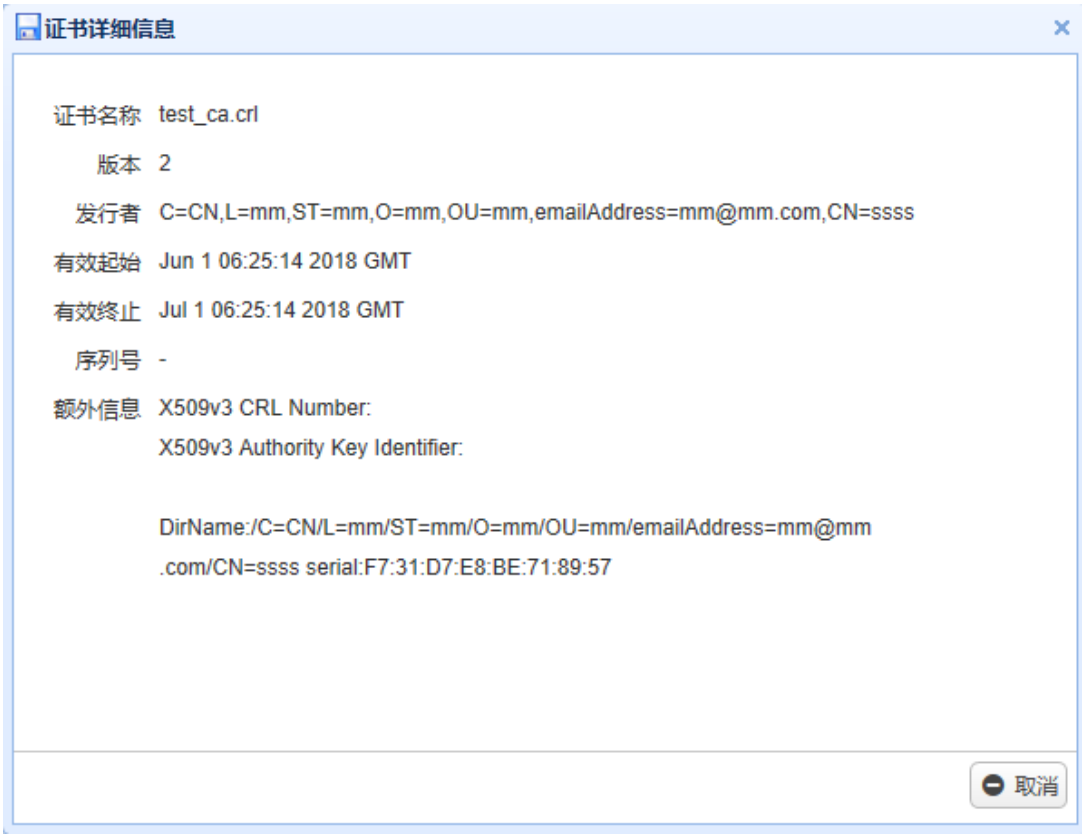
图1-12 本地 CRL 文件概览页面



点击<删除>按钮，可以删除选中的条目。

点击<详细信息>按钮，可以查看 CRL 的详细信息。如图 1-13 所示。

图1-13 查看本地 CRL 文件的详细信息



点击<导出>按钮，可以导出本地 CRL 文件。

1.5 国密证书

通过菜单“策略配置 > 对象管理 > 本地证书 > 证书 > 国密”，进入如图 1-14 所示页面。在该页面可以新建、编辑、删除、查看本地国密配置

图1-14 本地国密页面

点击<导入>按钮，导入国密证书，如图 1-15 所示。各个配置项的含义如表 1-4 所示。

图1-15 导入国密证书配置页面

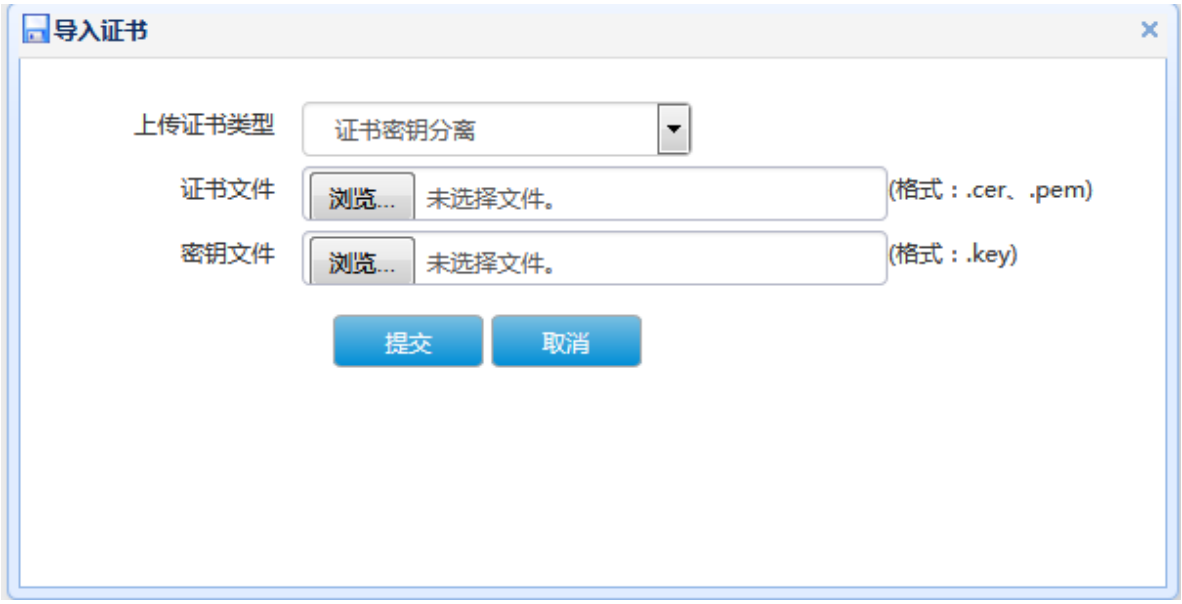


表1-4 导入国密证书各个配置项含义描述表

标题项	说明
上传证书类型	上传的CA证书文件，支持.cer、.pem格式的证书文件。
证书文件	证书密钥分离格式的证书文件。
密钥文件	证书密钥分离格式的密钥文件。

点击<提交>按钮，提交配置后，可以通过如图 1-16 所示的本地国密页面导出、查看、删除导入的CRL 文件。

图1-16 国密证书概览页面

点击<删除>按钮，可以删除选中的条目。

注意

国密证书不支持查看详细信息及导出，<详细信息>和<导出>按钮置灰。

1.6 自动获取CRL

通过菜单“策略配置 > 对象管理 > 本地证书 > 自动获取 CRL”，进入如图 1-17 所示页面。在该页面上，可以新建、编辑、删除、查看自动获取 CRL 配置。

图1-17 自动获取 CRL 文件页面

点击<新建>按钮，新建自动获取 CRL 配置，如图 1-18 所示。各个配置项的含义如表 1-5 所示。

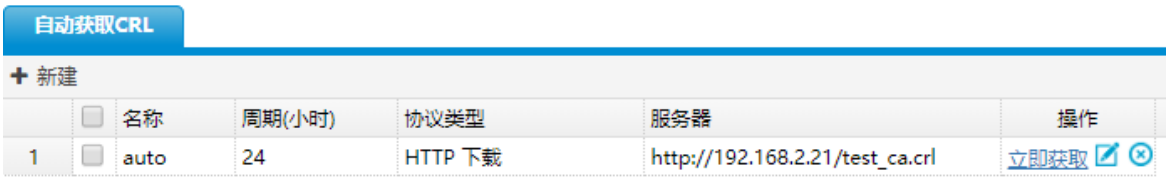
图1-18 新建自动获取 CRL 配置页面

表1-5 新建自动获取 CRL 各个配置项含义描述表

标题项	说明
名称	自动获取CRL文件的配置名称。
自动下载周期	自动获取CRL文件的周期。
协议类型	自动获取CRL使用的协议类型。
HTTP服务器URL	使用HTTP获取CRL时使用的URL。
LDAP服务器名称	使用LDAP获取CRL时使用的LDAP服务器名称。

点击<提交>按钮，提交配置后，可以通过如图 1-19 所示的页面编辑、删除、立即获取 CRL 文件。

图1-19 自动获取 CRL 文件配置概览页面



点击<编辑>按钮，可以编辑选中的条目。

点击<立即获取>按钮，可以立即从配置的服务器处获取 CRL 文件。

点击<删除>按钮，可以删除选中的条目。

注意

自动获取到的 CRL 文件将以配置条目名称命名。

1.7 典型配置举例

1.7.1 用户证书配置举例

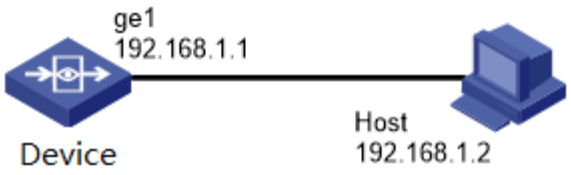
1. 组网需求

通过浏览器，向设备导入本地用户证书。

- Host 与设备网络可达。
- Host 上存在用户证书。

2. 组网图

图1-20 用户证书组网图

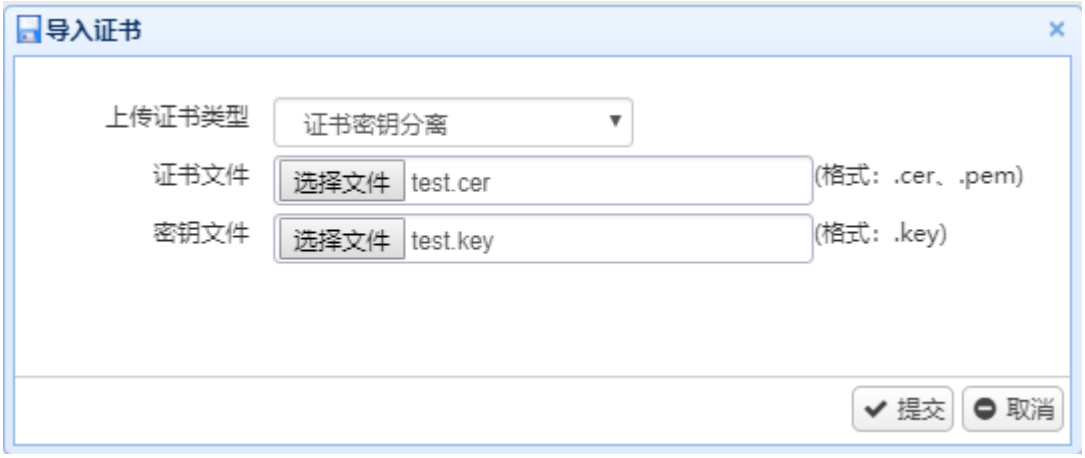


3. 配置步骤

(1) 按图 1-20 所示组网。

(2) 进入本地用户证书页面，点击<导入>按钮，进入如图 1-21 所示页面，选择上传文件。

图1-21 导入本地用户证书

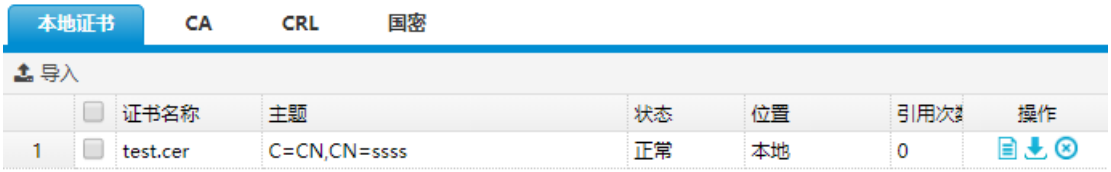


点击<提交>按钮，上传用户证书。

4. 验证配置

进入本地用户证书页面，查看上传的用户证书，如图 1-22 所示。

图1-22 查看上传的用户证书



1.7.2 自动获取 CRL 配置举例

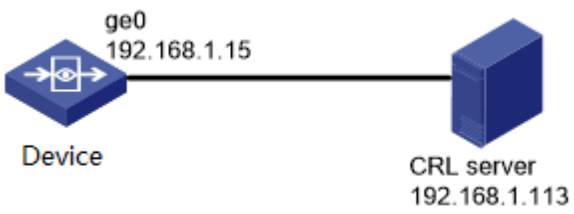
1. 组网需求

根据自动获取配置，从 CRL 服务器自动获取 CRL 文件。

- CRL 服务器与设备网络可达。
- CRL 服务器上存在 CRL 证书。

2. 组网图

图1-23 自动获取 CRL 配置组网图



3. 配置步骤

(1) 按图 1-23 所示组网。

(2) 进入自动获取 CRL 配置页面，配置自动获取 CRL。如图 1-24 所示。

图1-24 自动获取 CRL 配置

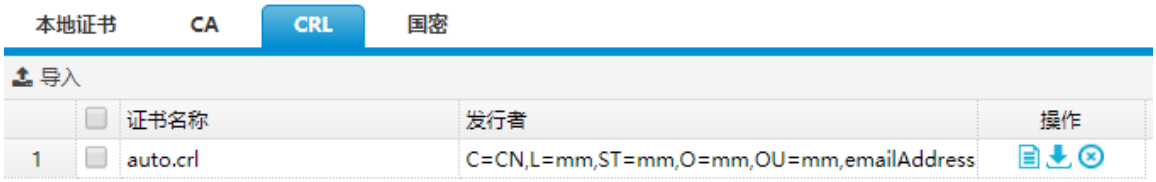
点击<提交>按钮，提交配置。

(3) 点击<立即获取>按钮，立刻获取 CRL 文件。

4. 验证配置

进入本地 CRL 页面，查看自动获取的 CRL 文件。如图 1-25 所示。

图1-25 自动获取 CRL 文件



目 录

1 审计策略 ····· 1-1
1.1 审计策略概述 ····· 1-1
1.2 配置审计策略 ····· 1-1
1.3 启用禁用审计策略 ····· 1-4
1.4 复制审计策略 ····· 1-5
1.5 审计策略优先级配置 ····· 1-5
1.6 审计策略查询 ····· 1-6
1.7 审计策略典型配置举例 ····· 1-7
1.7.1 组网需求 ····· 1-7
1.7.2 组网图 ····· 1-8
1.7.3 配置步骤 ····· 1-8
1.7.4 验证配置 ····· 1-10

1 审计策略

1.1 审计策略概述

审计策略是基于用户上网行为进行审计，审计从 HTTP、邮件、即时通讯、基础协议、娱乐股票、网络应用等 6 大维度进行审计。

本功能具有如下功能点：

- 审计策略可单独支持增、删、改、查、启用、禁用、优先级调整。
- 审计策略目前基于应用行为进行审计，不再基于应用或应用组进行审计，配置逻辑简单清晰。
- 审计策略适用于 IPv4 和 IPv6 网络的审计。

说明

- 如果未开启 https 解密功能，系统默认只对内置的 https 网站访问进行审计，可以通过 **https audit all** 命令设置对所有的 https 网站访问进行审计，但是开启后可能会产生大量的审计日志。建议使用默认配置（**https audit predefine**），如需对加密的网站进行审计，可配合 https 解密策略进行审计。
- 对于一些加密的应用行为需要在设备上配置HTTPS解密策略，优先进行HTTPS解密，解密之后再审计；如未开启解密，则加密的应用行为将不会进行审计。
- 网络应用类的应用行为审计是需要有登录账号或评论等操作才会产生相应的日志，只是访问页面查询将不会进行审计。

1.2 配置审计策略

通过菜单“策略配置 > 审计策略”，进入审计策略显示页面，如图 1-1 所示。审计策略页面显示项含义如表 1-1 所示。

图1-1 审计策略显示页面

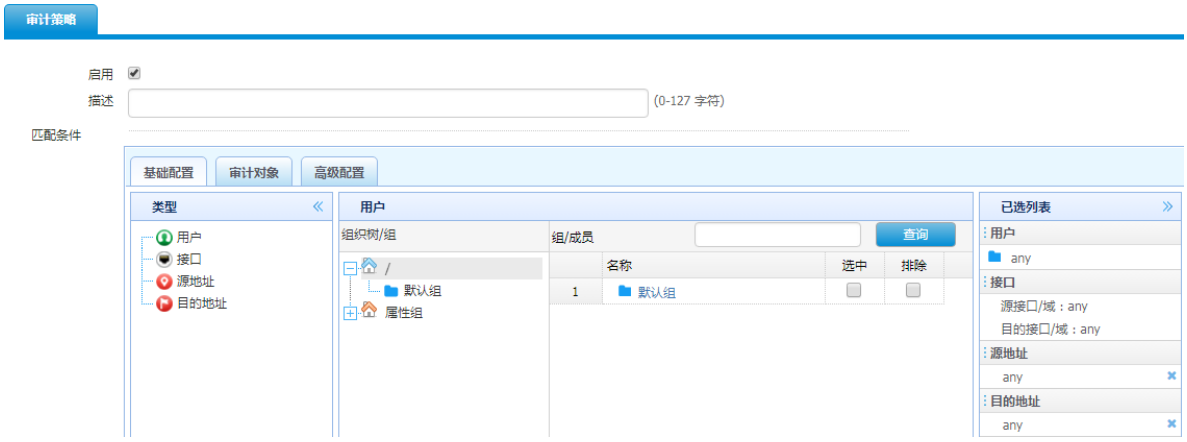
表1-1 审计策略显示页面含义表

标题项	说明
状态	策略的状态： • 表示策略启用和时间生效；

	• 表示策略禁用和时间失效。
ID	审计策略ID。
用户	匹配审计策略的用户对象，可以在策略外点进去单独进行编辑。
源接口/域	匹配审计策略的源接口/域，可以在策略外点进去单独进行编辑。
目的接口/域	匹配审计策略的目的接口/域，可以在策略外点进去单独进行编辑。
源地址	匹配审计策略的源地址，可以在策略外点进去单独进行编辑。
目的地址	匹配审计策略的目的地址，可以在策略外点进去单独进行编辑。
终端	匹配审计策略的终端类型。
描述	审计策略描述。
匹配次数	匹配审计策略的次数。
审计对象	匹配审计策略的审计对象。
时间	匹配审计策略的时间对象。
操作	修改：对当前审计策略进行编辑修改操作。 删除：对当前审计策略进行删除操作。

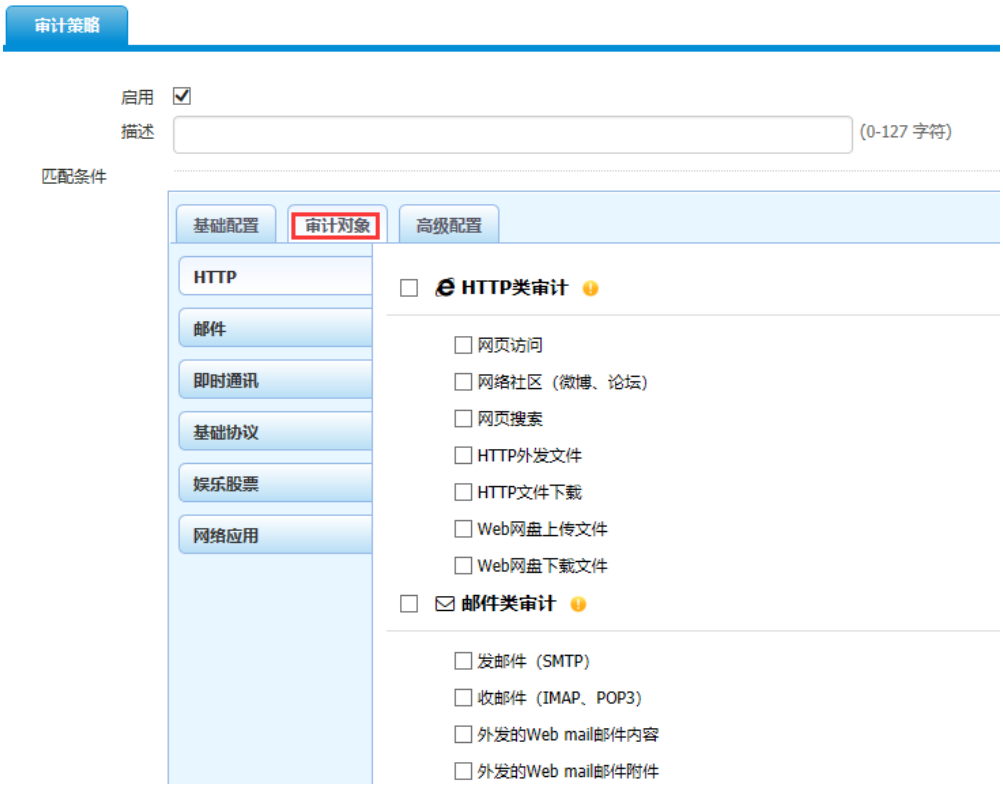
单击<新建>按钮，进入审计策略配置页面，如图 1-2 所示。

图1-2 审计策略基础配置页面



单击“审计对象”标签页，进入审计对象配置页面，如图 1-3 所示。

图1-3 审计策略审计对象配置页面



单击“高级配置”标签页，进入高级配置页面，如图 1-4 所示。

图1-4 审计策略高级配置

审计策略详细配置含义如表 1-2 所示。

表1-2 审计策略详细配置

标题项	说明
启用	新建策略默认勾选该项，表示策略启用；不勾选表示禁用状态。
描述	审计策略描述。
用户	匹配审计策略的用户对象。
接口	匹配审计策略的源目的接口/域。
源地址	匹配审计策略的源地址。
目的地址	匹配审计策略的目的地址。
HTTP	HTTP类审计对象，可以对HTTP类行为进行审计，主要包括网页访问、网络社区、网页搜索、HTTP文件上传下载、web网盘文件上传下载审计。
邮件	邮件类审计对象，可以对邮件类行为进行审计，主要包括SMTP、POP3、IMAP、Webmail收发邮件及附件审计。
即时通讯	即时通讯类审计对象，主要包括常用通讯软件QQ、微信、飞信等登录账号审计，以及收发消息行为审计，还有其它类通讯软件登录行为审计。
基础协议	基础协议类审计对象，主要包括FTP登录上传下载文件审计。
娱乐股票	娱乐股票类审计对象，主要包括娱乐股票类应用登录账号以及评论类审计。
网络应用	网络应用类审计对象，主要包括出上面具体应用行为外的其它一些应用行为进行审计。
时间	匹配审计策略的时间对象。
日志级别	审计策略日志记录级别，默认是信息级别，可以根据需求配置日志级别。
终端	匹配审计策略终端类型，默认是any所有终端类型，可以根据需求配置终端类型进行审计。
终端型号	选择终端型号，默认为any。此功能依赖于第三方用户同步中的ddi终端用户功能，需要将终端型号信息同步给设备。

1.3 启用禁用审计策略

通过菜单“策略配置 > 审计策略”，进入审计策略显示页面，如图 1-5 所示。

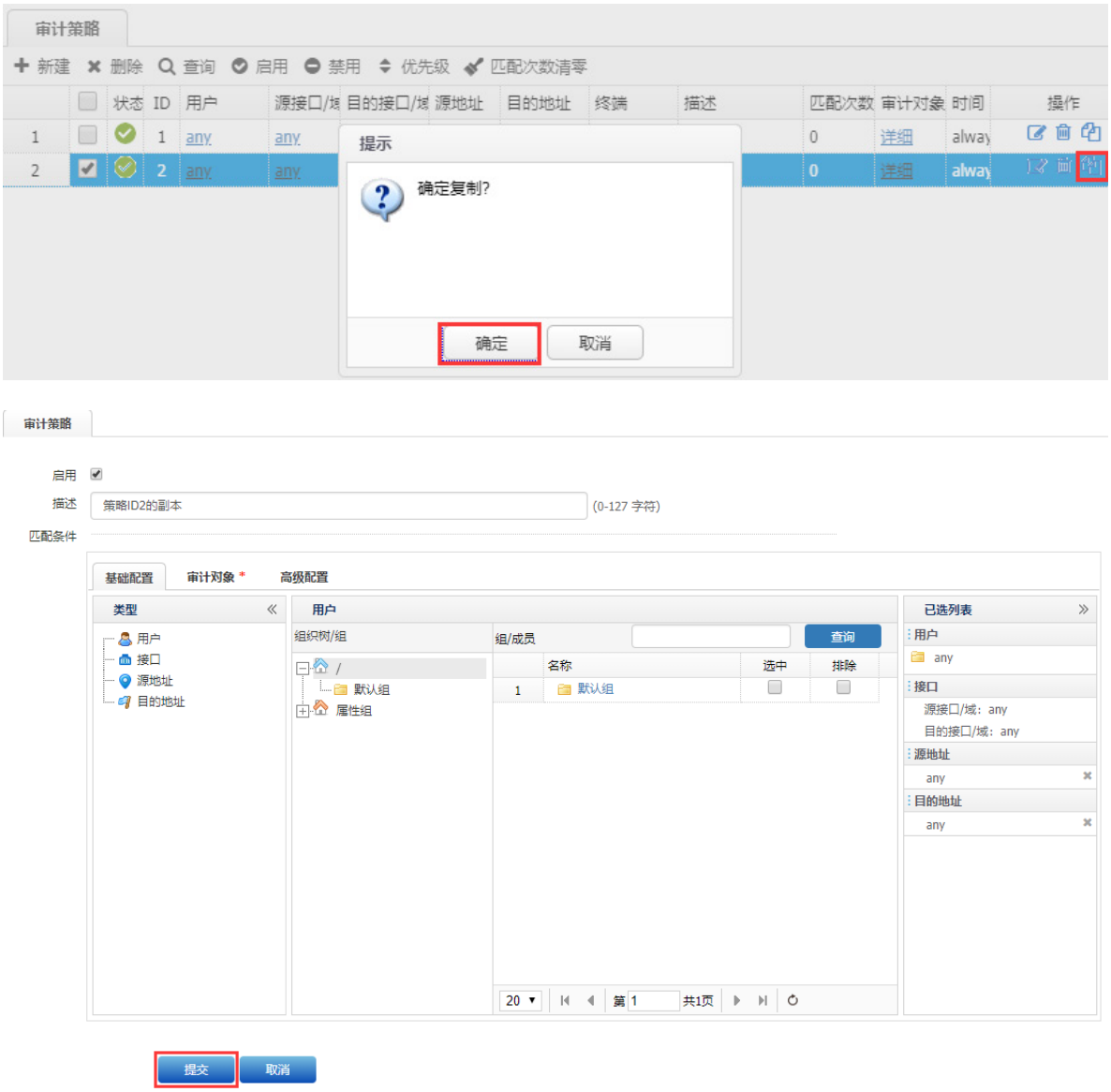
勾选要启用或者禁用的审计策略，单击<启用>按钮或<禁用>按钮可以启动和禁用该审计策略。

图1-5 审计策略启用禁用

1.4 复制审计策略

通过菜单“策略配置 > 审计策略”，进入审计策略显示页面。单击需要复制的审计策略后面的 按钮，然后单击“确定”按钮，进入复制后的策略编辑页面，最后点“提交”按钮即可以对该审计策略进行复制，生成一个新的审计策略。

图1-6 审计策略复制



1.5 审计策略优先级配置

通过菜单“策略配置 > 审计策略”，进入审计策略显示页面，选择需要调整的审计策略，点击<优先级>按钮，进入审计策略优先级配置页面，如图 1-6 所示。

图1-7 审计策略优先级配置

审计策略优先级详细配置说明，如表 1-3 所示。

表1-3 审计策略优先级配置

标题项	说明
被移动的策略ID	被移动的策略ID。
目标位置	移动后的位置： • 策略最前指移动到所有策略的最前面。 • 策略 ID 之前指移动到某条固定的策略之前。 • 策略 ID 之后指移动到某条固定的策略后面。 • 策略最后指移动到所有策略的后面。
目标位置策略ID	参考策略ID。

1.6 审计策略查询

通过菜单“策略配置 > 审计策略”，进入审计策略显示页面，点击<查询>按钮，进入审计策略查询页面，如图 1-7 所示。

图1-8 审计策略查询

审计策略查询项查询条件说明，如表 1-4 所示。

表1-4 审计策略查询

标题项	说明
匹配ID	被搜索的策略ID。
源接口/域	策略所选择的源接口/域。
源地址	策略所配置包含该地址的地址对象（可基于地址对象、IP地址、域名搜索）。
用户	策略所选择的用户。
目的接口/域	策略所选择的目的接口/域。
目的地址	策略所配置包含该地址的地址对象（可基于地址对象、IP地址、域名搜索）。
描述	策略所对应的描述信息。

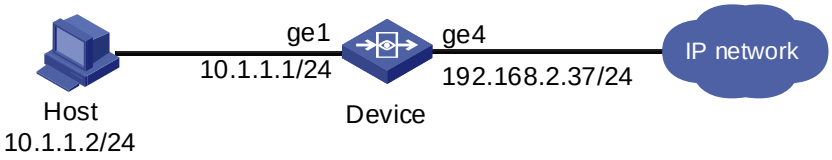
1.7 审计策略典型配置举例

1.7.1 组网需求

内网用户通过设备访问外网，工作时间（9:00-18：00）现需对内网用户访问外网的所有行为进行审计。

1.7.2 组网图

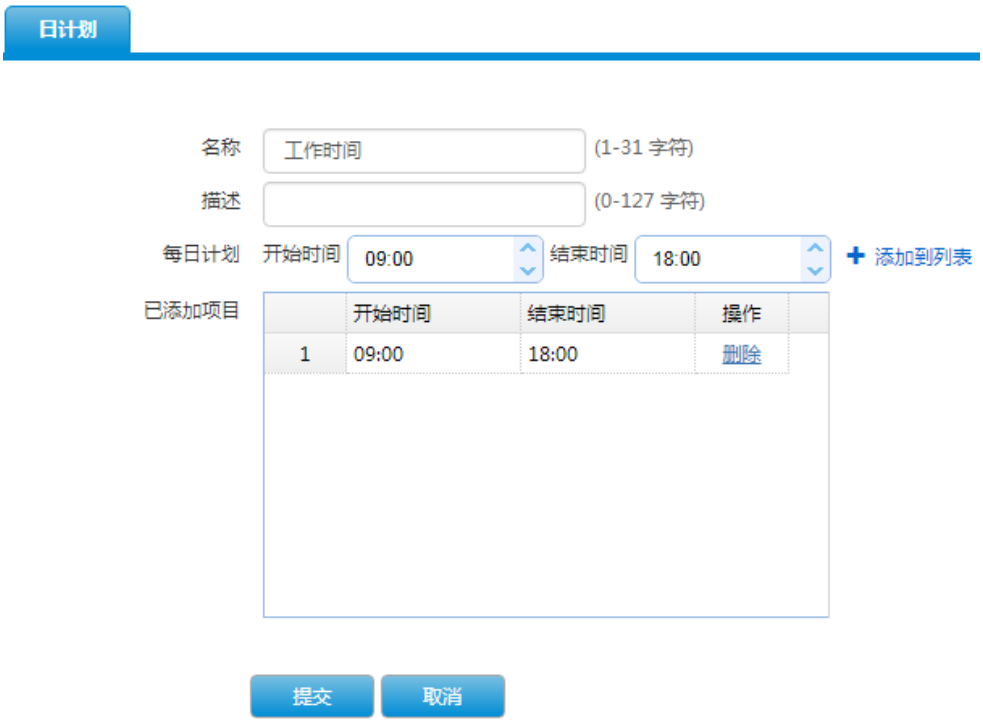
图1-9 审计策略配置举例组网图



1.7.3 配置步骤

(1) 配置时间对象。通过菜单“策略配置>对象管理>时间对象>日计划”，点击<新建>按钮，进入日计划配置页面，如图 1-10 所示。

图1-10 配置时间对象



点击<提交>按钮，提交日计划时间对象配置，如图 1-11 所示。

图1-11 日计划时间对象配置

(2) 配置审计策略。通过菜单“策略配置 > 审计策略”，点击<新建>按钮，进入审计策略配置页面，匹配条件按默认配置，如图 1-12 所示，审计对象选择所有，如图 1-13 所示，高级配置中时间对象选择配置的时间对象，如图 1-13 所示。

图1-12 审计策略基础配置

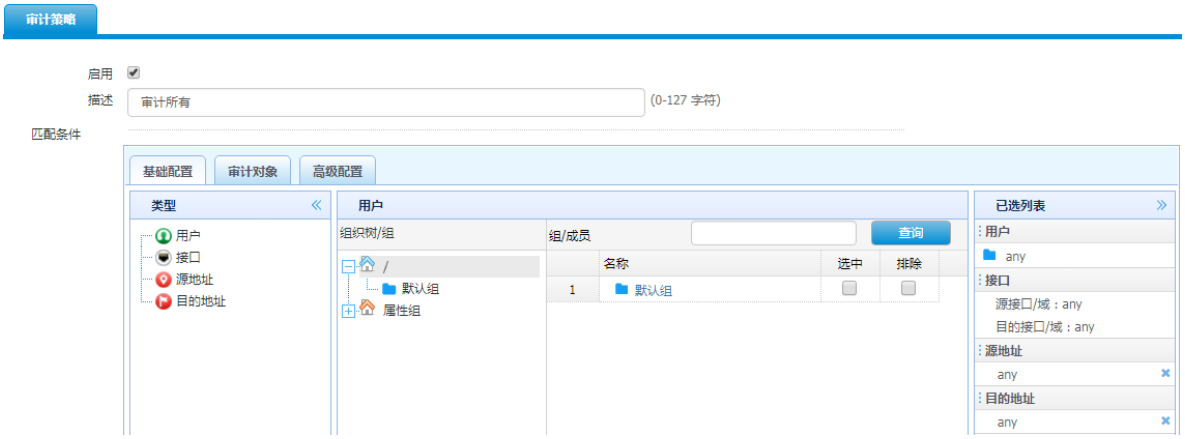


图1-13 审计策略审计对象配置

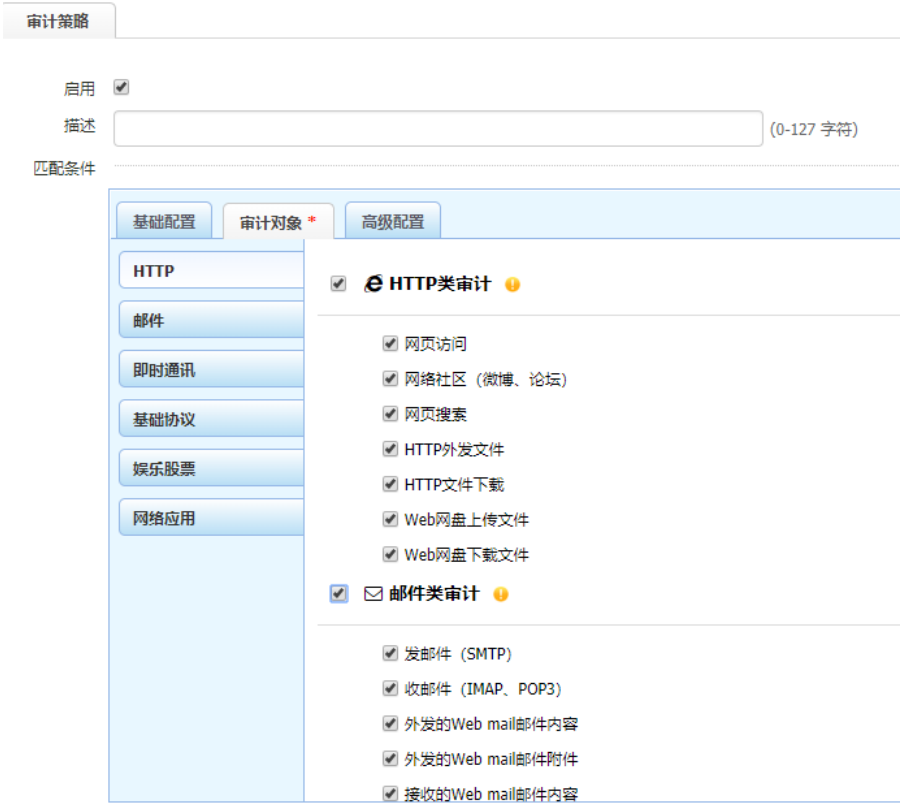


图1-14 审计策略高级配置

点击策略下方的<提交>按钮，审计策略配置完成，如图[图 1-15]所示。

图1-15 审计策略配置

1.7.4 验证配置

配置完成后，内网用户在工作时间段（9:00-18:00）访问外网的上网行为均被审计到，工作时间外访问外网将不进行审计。

目 录

1 控制策略 ····· 1-1

1.1 控制策略 ····· 1-1

1.1.1 控制策略概述 ····· 1-1

1.1.2 控制策略配置 ····· 1-1

1.1.3 控制策略优先级配置 ····· 1-4

1.1.4 启用和禁用控制策略 ····· 1-5

1.1.5 复制控制策略 ····· 1-6

1.1.6 删除控制策略 ····· 1-6

1.1.7 清除控制策略匹配计数 ····· 1-7

1.1.8 控制策略默认规则 ····· 1-7

1.1.9 控制策略查询 ····· 1-7

1.1.10 策略分组 ····· 1-8

1.1.11 控制策略配置案例 ····· 1-9

1.1.12 IPv6 控制策略配置举例 ····· 1-12

1.2 WEB 关键字过滤 ····· 1-17

1.2.1 WEB 关键字过滤概述 ····· 1-17

1.2.2 WEB 关键字页面 ····· 1-17

1.2.3 搜索引擎规则 ····· 1-19

1.2.4 HTTP 上传规则 ····· 1-20

1.2.5 网页内容规则 ····· 1-21

1.2.6 WEB 关键字过滤配置案例 ····· 1-23

1.3 URL 过滤 ····· 1-29

1.3.1 URL 过滤概述 ····· 1-29

1.3.2 URL 过滤策略页面 ····· 1-29

1.3.3 恶意 URL 页面 ····· 1-30

1.3.4 URL 过滤配置案例 ····· 1-31

1.3.5 DNS 过滤配置案例 ····· 1-32

1.4 应用控制 ····· 1-35

1.4.1 应用控制概述 ····· 1-35

1.4.2 应用控制页面 ····· 1-35

1.4.3 应用控制配置案例 ····· 1-36

1.5 邮件控制 ····· 1-38

1.5.1 概述 ····· 1-38

1.5.2 邮件控制 ····· 1-38
1.5.3 邮件控制配置举例 ····· 1-39
1.6 虚拟账号 ····· 1-44
1.6.1 概述 ····· 1-44
1.6.2 配置虚拟账号 ····· 1-44
1.6.3 虚拟账号配置举例 ····· 1-44
1.7 文件类型过滤 ····· 1-52
1.7.1 文件类型过滤简介 ····· 1-52
1.7.2 文件类型过滤使用限制 ····· 1-52
1.7.3 文件类型过滤页面 ····· 1-52
1.7.4 文件类型过滤配置举例 ····· 1-54
1.8 终端公告推送 ····· 1-56
1.8.1 终端公告推送简介 ····· 1-56
1.8.2 终端公告推送页面 ····· 1-56
1.8.3 终端公告配置举例 ····· 1-57
1.9 高级配置 ····· 1-63
1.9.1 高级配置简介 ····· 1-63
1.9.2 高级配置页面 ····· 1-63
1.9.3 终端控制配置举例 ····· 1-64

1 控制策略

1.1 控制策略

1.1.1 控制策略概述

控制策略对通过设备的用户、源接口/域、目的接口/域、源地址、目的地址、应用、服务、终端、时间等维度进行访问控制，针对应用、URL、入侵防御、病毒防护等内容进行统一管控，并且支持策略分组。

控制策略适用于 IPv4 和 IPv6 网络的访问控制。

1.1.2 控制策略配置

在导航栏中选择“策略配置 > 控制策略”，进入控制策略显示界面，如图 1-1 所示。

图1-1 控制策略显示界面

控制策略的含义如表 1-1 所示：

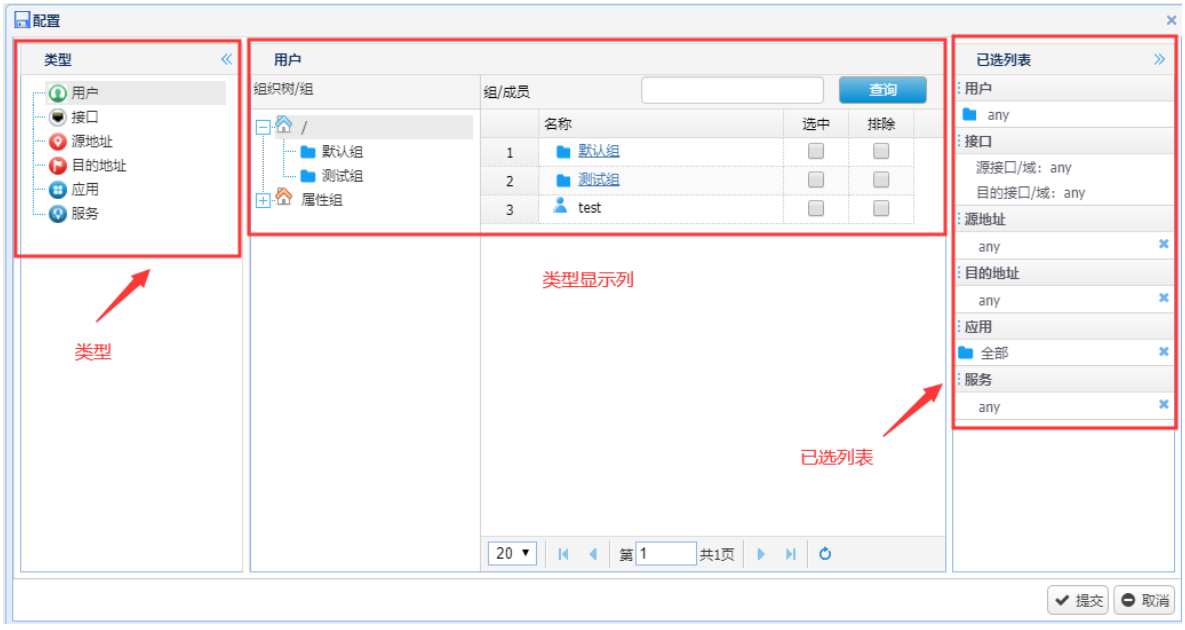
表1-1 控制策略显示信息描述表

标题项	说明
状态	控制策略的状态： • 表示策略启用 • 表示策略禁用
ID	控制策略的ID。
用户	匹配控制策略的用户对象。
行为	控制策略行为的状态包含： • 允许 • 拒绝
策略组	策略所属的分组名称。
源接口/域	匹配控制策略的源接口/域。
目的接口/域	匹配控制策略的目的接口/域。
源地址	匹配控制策略的源地址。
目的地址	匹配控制策略的目的地址。

标题项	说明
应用	匹配控制策略的应用对象。
服务	匹配控制策略的服务对象。
终端	匹配控制策略匹配的终端类型，包括：any、移动终端、PC、多终端。 移动终端：基于Android或IOS系统的智能手机或Pad； PC：基于Windows操作系统的PC或笔记本； 多终端：单个IP下同时存在电脑和移动终端。
描述	控制策略描述。
匹配次数	匹配控制策略的次数。
应用安全	如果显示图标，表示已经配置应用过滤或URL过滤规则。
时间	匹配控制策略匹配的时间对象。
日志	设备是否记录syslog格式的控制策略日志。
老化时间	基于控制策略的老化时间，缺省情况下，老化时间为0，表示使用各个协议默认的老化时间。
操作	控制策略支持的操作，包含编辑和删除。

策略支持外部编辑，在导航栏中选择“策略配置 > 控制策略”，进入控制策略页面，点击任一支持外部编辑的 7 元组对象：用户、源接口/域、目的接口/域、源地址、目的地址、应用、服务，如图 1-2 所示。

图1-2 策略外部编辑配置界面



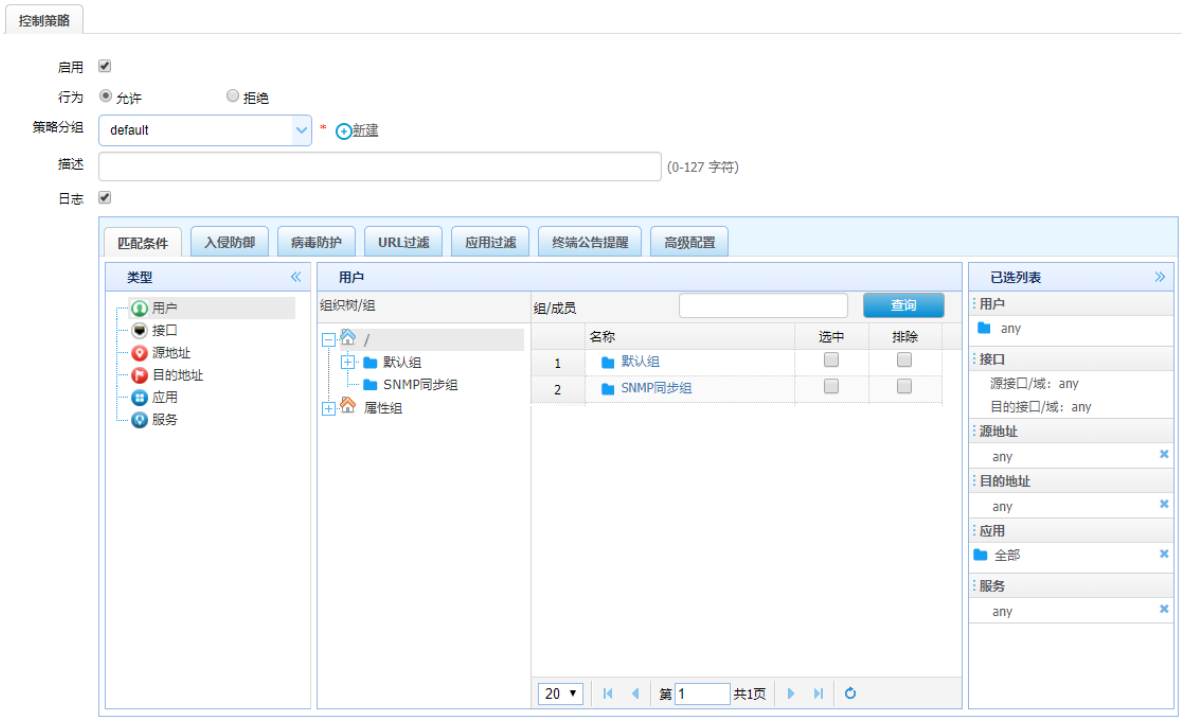
策略外部编辑界面的详细信息如表 1-2 所示：

表1-2 策略外部编辑界面详细信息

标题项	说明
类型	类型包含：用户、接口、源地址、目的地址、应用、服务
类型显示列	点击相应类型后，此列显示对应的类型数据，可直接选择进行配置。
已选列表	已配置类型的对象内容显示区。

单击<新建>按钮，进入控制策略配置页面，如下图所示。

图1-3 控制策略配置界面



控制策略详细配置说明，如表 1-3 所示。

表1-3 控制策略详细配置

标题项	说明
启用	策略启用和禁用，勾选表示开启策略，不勾选表示禁用策略。
行为	策略的行为包含： • 允许，对匹配条件的会话进行应用控制，如 URL 过滤和应用过滤。 • 拒绝，阻断命中匹配条件的会话。
策略分组	策略可以分组展示。
日志	勾选后，设备会记录syslog格式的控制策略日志。在“系统管理>系统设定>日志设定”页面，可以设置是否将指定级别的控制策略日志发送到日志服务器。

标题项	说明
描述	控制策略描述信息。
匹配条件	控制策略的匹配条件，包含用户、接口、源地址、目的地址、应用、服务。
入侵防御	入侵防御配置，包括事件集等。
病毒防护	病毒防护配置，包括防护项目等。
URL过滤	URL过滤规则，包含URL控制和恶意URL控制。
应用过滤	应用过滤规则，包含应用控制、邮件控制、WEB关键字控制、虚拟账号控制。
终端公告提醒	给匹配条件的终端推送公告提醒页面。策略首次下发后会进行第一次推送，后续按间隔定期推送。
高级配置	包含时间对象配置、老化时间配置、终端、终端型号配置。

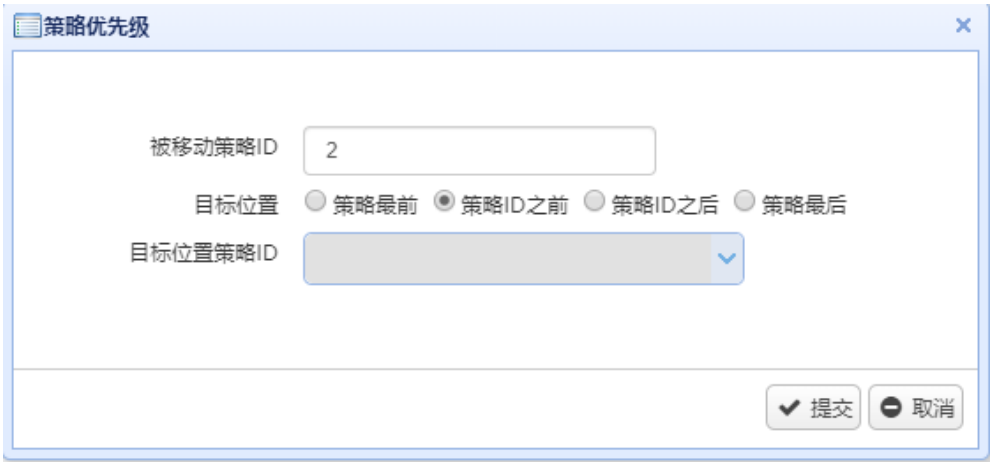
说明

- 控制策略动作为“拒绝”时，如果勾选了“日志”，设备只记录 syslog 格式的控制策略日志，不记录本地日志。如果需要在本地记录日志，可将控制策略的行为配置为“允许”，在应用过滤中配置处理动作为“拒绝”的策略，设备匹配到该策略后会在本地产生相应的日志。
- 控制策略动作为“允许”时，设备 syslog 日志支持记录级别为“info”的控制策略日志，在设置日志外发级别需要选择“全部级别”，或者“信息”，或者“调试”，远端 syslog 服务器才能收到日志。
- 控制策略动作为允许的时候，建议不要勾选“日志”。如果勾选日志并外发，会产生大量外发日志，可能会对设备性能产生影响。

1.1.3 控制策略优先级配置

在导航栏中选择“策略配置 > 控制策略”，单击<优先级>按钮进入控制策略优先级配置页面，如图 1-4 所示。

图1-4 策略优先级



控制策略优先级详细配置说明，如表 1-4 所示。

表1-4 控制策略优先级详细配置

标题项	说明
被移动的策略ID	被移动的策略索引。
目标位置	移动后的位置： • 策略最前指移动到所有策略的最前面。 • 策略 ID 之前指移动到某条固定的策略之前。 • 策略 ID 之后指移动到某条固定的策略之后。 • 策略最后指移动到所有策略的后面。
目标位置策略ID	参考策略索引，可以选择对应策略ID，将当前策略移动到该策略ID之前或之后。

1.1.4 启用和禁用控制策略

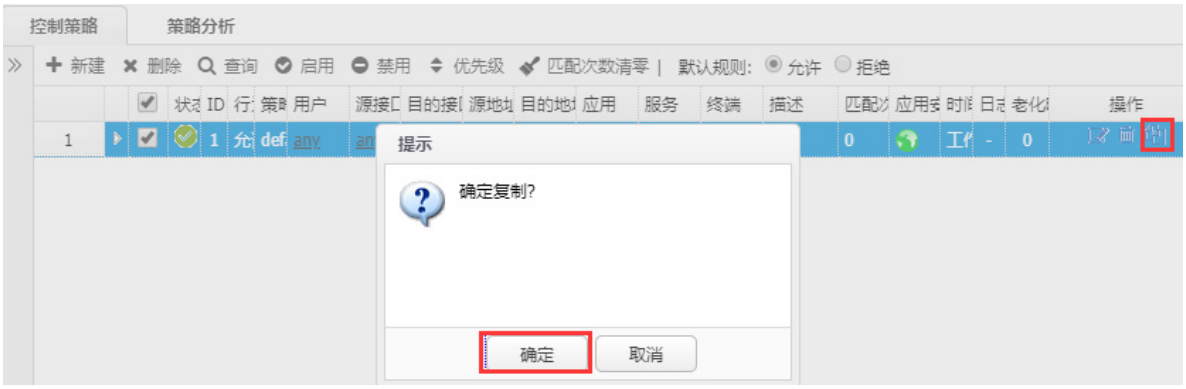
在导航栏中选择“策略配置 > 控制策略”，进入控制策略显示页面，如图 1-5 所示。勾选要启用或者禁用的控制策略，单击<启用>或<禁用>按钮可以启动和禁用该控制策略。

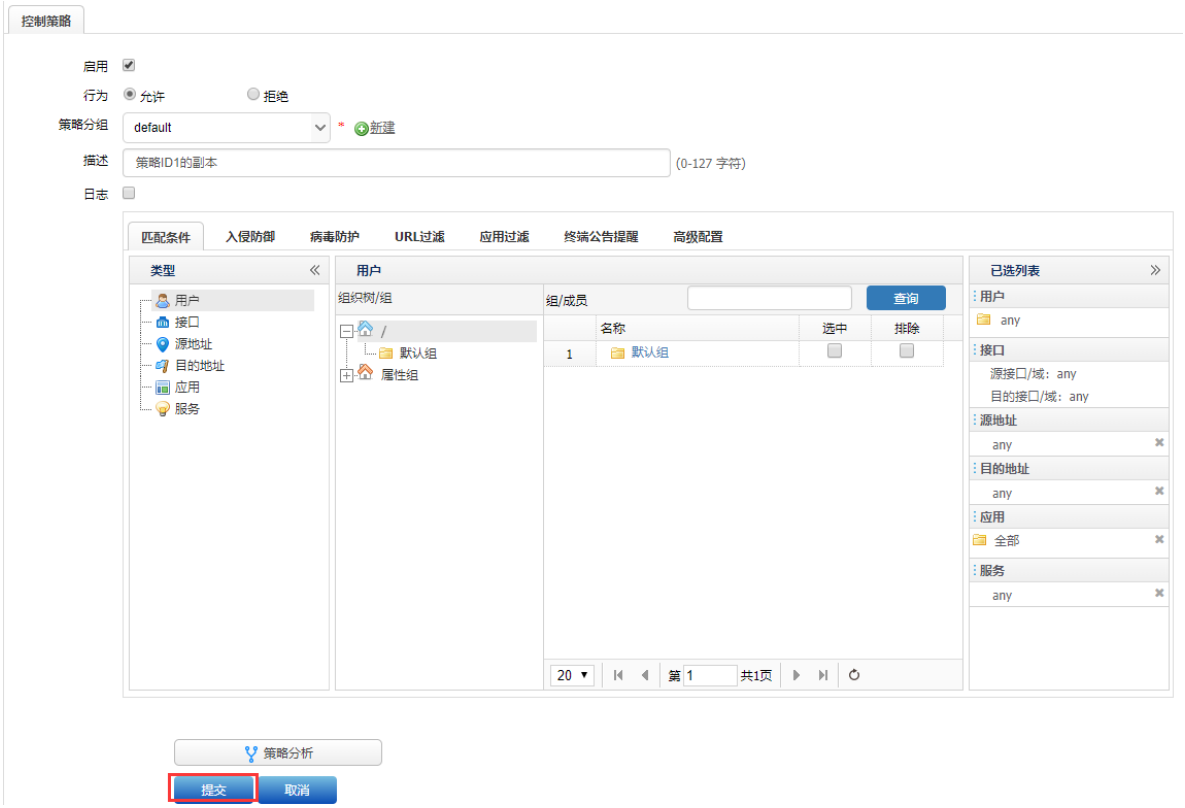
图1-5 控制策略启用和禁用

1.1.5 复制控制策略

在导航栏中选择“策略配置 > 控制策略”，进入控制策略显示页面。单击需要复制的控制策略后面的按钮，然后单击“确定”按钮，进入复制后的策略编辑页面，最后单击“提交”按钮即可以对该控制策略进行复制，生成一个新的控制策略。

图1-6 复制控制策略





1.1.6 删除控制策略

在导航栏中选择“策略配置 > 控制策略”，进入控制策略显示页面，如图 1-7 所示。勾选要删除的控制策略，单击<删除>按钮或点击操作中<删除>按钮，可以删除该控制策略。

图1-7 控制策略删除

1.1.7 清除控制策略匹配计数

在导航栏中选择“策略配置 > 控制策略”，进入控制策略显示页面，如图 1-8 所示。勾选要清除匹配计数的控制策略，单击<匹配次数清零>按钮可以清除该控制策略的匹配计数。

图1-8 清除控制策略匹配计数

1.1.8 控制策略默认规则

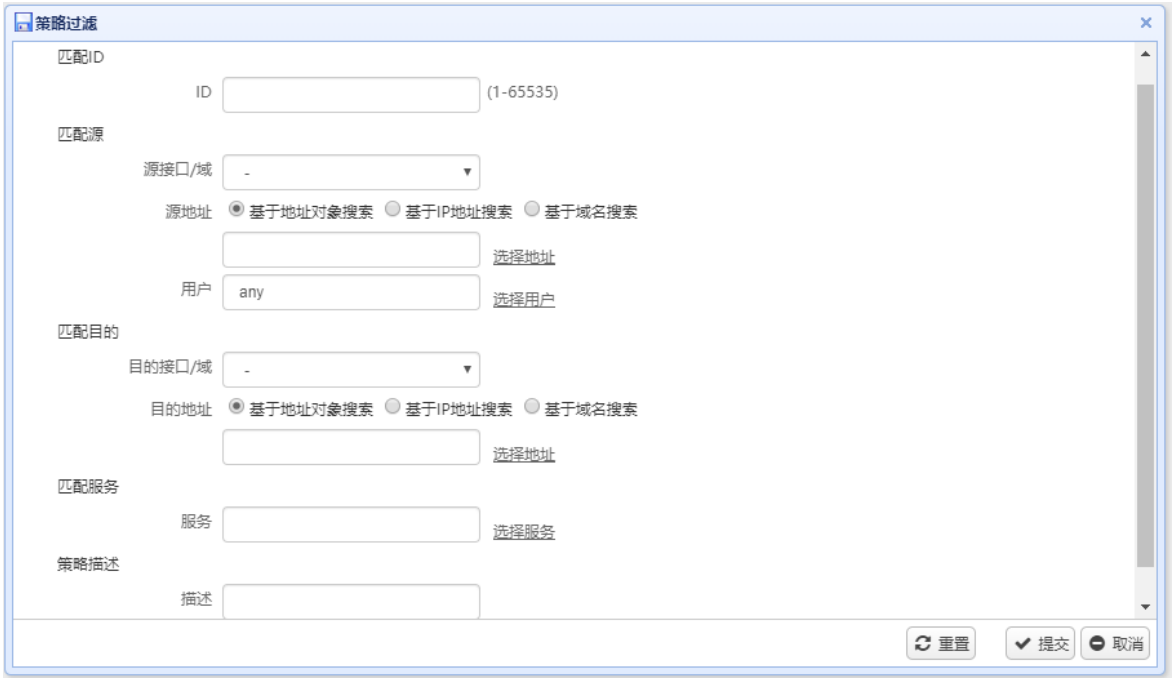
在导航栏中选择“策略配置 > 控制策略”，进入控制策略显示页面，如图 1-9 所示。勾选允许或拒绝单选框，可以修改默认控制策略行为。

图1-9 默认规则

1.1.9 控制策略查询

在导航栏中选择“策略配置 > 控制策略”，进入控制策略显示页面，如图 1-10 所示。单击查询，填写过滤条件可以查询出符合该过滤条件的控制策略。

图1-10 控制策略查询



控制策略查询配置详细说明，如表 1-5 所示。

表1-5 控制策略查询详细配置

标题项	说明
ID	被查询的策略索引。
源接口/域	策略所选择的源接口。
源地址	策略所配置包含该地址的地址对象（可基于地址对象、IP地址和域名查询）。
用户	策略所选择的用户。
目的接口/域	策略所选择的目的接口。
目的地址	策略所配置包含该地址的地址对象（可基于地址对象、IP地址搜寻和域名查询）。
服务	策略所选择的服务。
描述	策略所对应的描述信息。

1.1.10 策略分组

在导航栏中选择“策略配置>控制策略”，进入控制策略显示页面，如图 1-11 所示。移动到左边，点击 »，会弹出策略分组管理页面。

图1-11 策略分组页面

策略分组详细说明，如表 1-6 所示。

表1-6 策略分组详细配置

标题项	说明
	新建策略分组。
	修改策略分组名称。
	删除策略分组。

1.1.11 控制策略配置案例

1. 组网需求

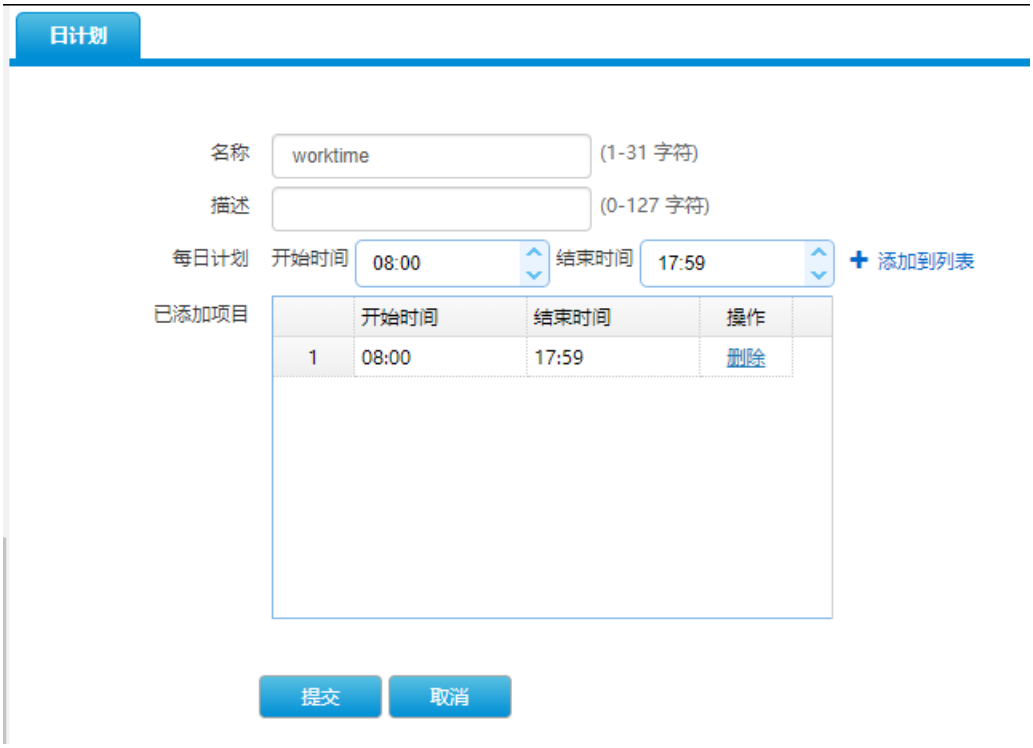
禁止公司员工上班时间（8：00—18：00）访问 QQ。

2. 配置步骤

(1) 配置日计划

在导航栏中选择“策略配置 > 对象管理 > 时间对象> 日计划”，单击<新建>按钮，进入日计划配置页面，如图 1-12 所示。

图1-12 日计划配置

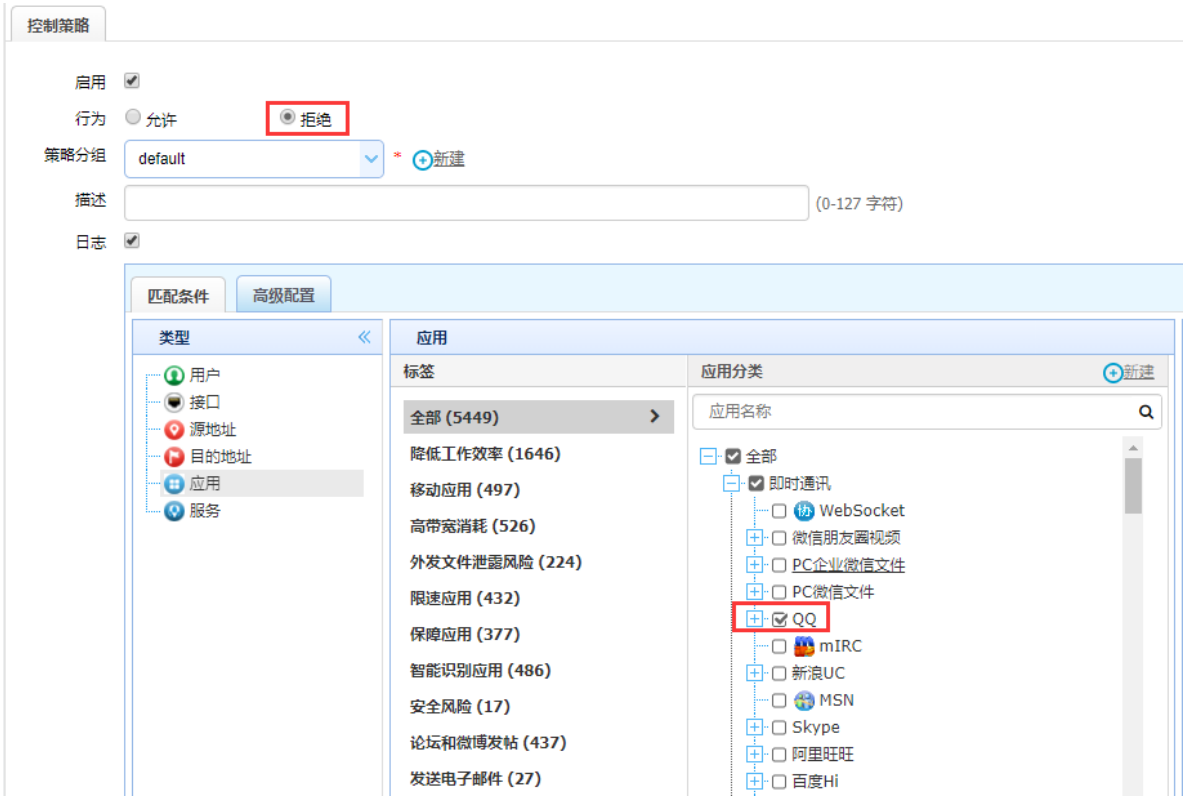


点击<提交>按钮，提交配置。

(2) 配置控制策略

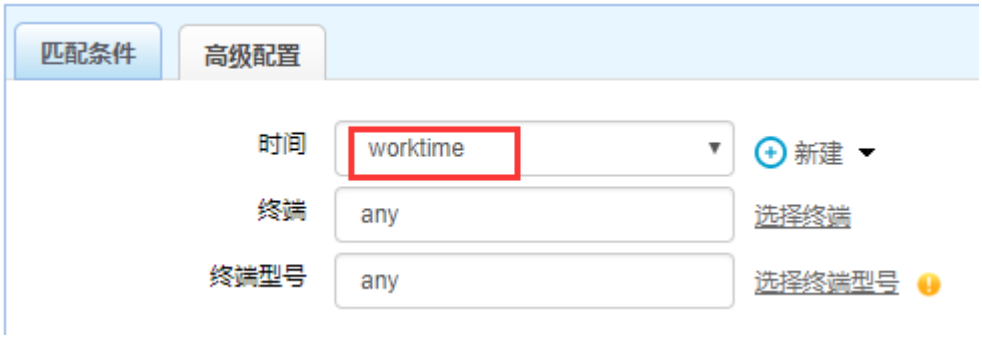
在导航栏中选择“策略配置 > 控制策略”，单击<新建>按钮，进入控制策略配置页面，行为选择拒绝，勾选日志，在“匹配条件”页面中，应用类型选择“即时通讯 > QQ”，如下图所示。

图1-13 控制策略配置



单击选择“高级配置”标签页，时间选择已配置的时间对象，如图 1-14 所示。

图1-14 控制策略高级配置



3. 验证配置

配置完成后，公司员工在 8：00—18：00 的时间范围内无法登录 QQ，但在其它时间是可以登录的。

1.1.12 IPv6 控制策略配置举例

1. 简介

控制策略不仅适用于 IPv4 网络，也同样适用于 IPv6 网络的，可以对通过设备的源接口，目的接口，源 IPv6 地址，目的 IPv6 地址，服务，用户，以及应用七元组进行访问控制。

说明

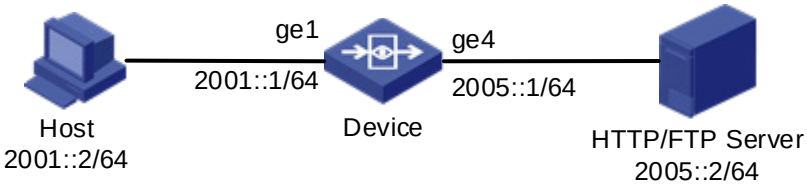
- 匹配基于 IPv6 的控制策略，用户识别范围需要配置为 any 或者识别方式配置为启发模式。
- 匹配基于 IPv6 的控制策略，需要在命令行启用 IPv6 enable 功能。

2. 组网需求

内网用户通过设备访问远端服务器，通过控制策略禁止内网用户访问远端 IPv6 的 HTTP 服务器和 FTP 服务器。

3. 组网图

图1-15 IPv6 控制策略组网图



4. 配置步骤

(1) 配置基于 IPv6 地址对象。

进入“策略配置>对象管理>地址对象”页面，新建一条地址对象。

图1-16 新建 IPv6 地址对象

(2) 配置基于 IPv6 的 URL 控制策略。

进入“策略配置>控制策略”页面，新建一条控制策略，在 URL 过滤策略中新建一条 URL 控制策略，URL 分类选择其它类，处理动作选择拒绝，日志级别配置通知，提交策略。

图1-17 新建控制策略-新建 URL 控制策略

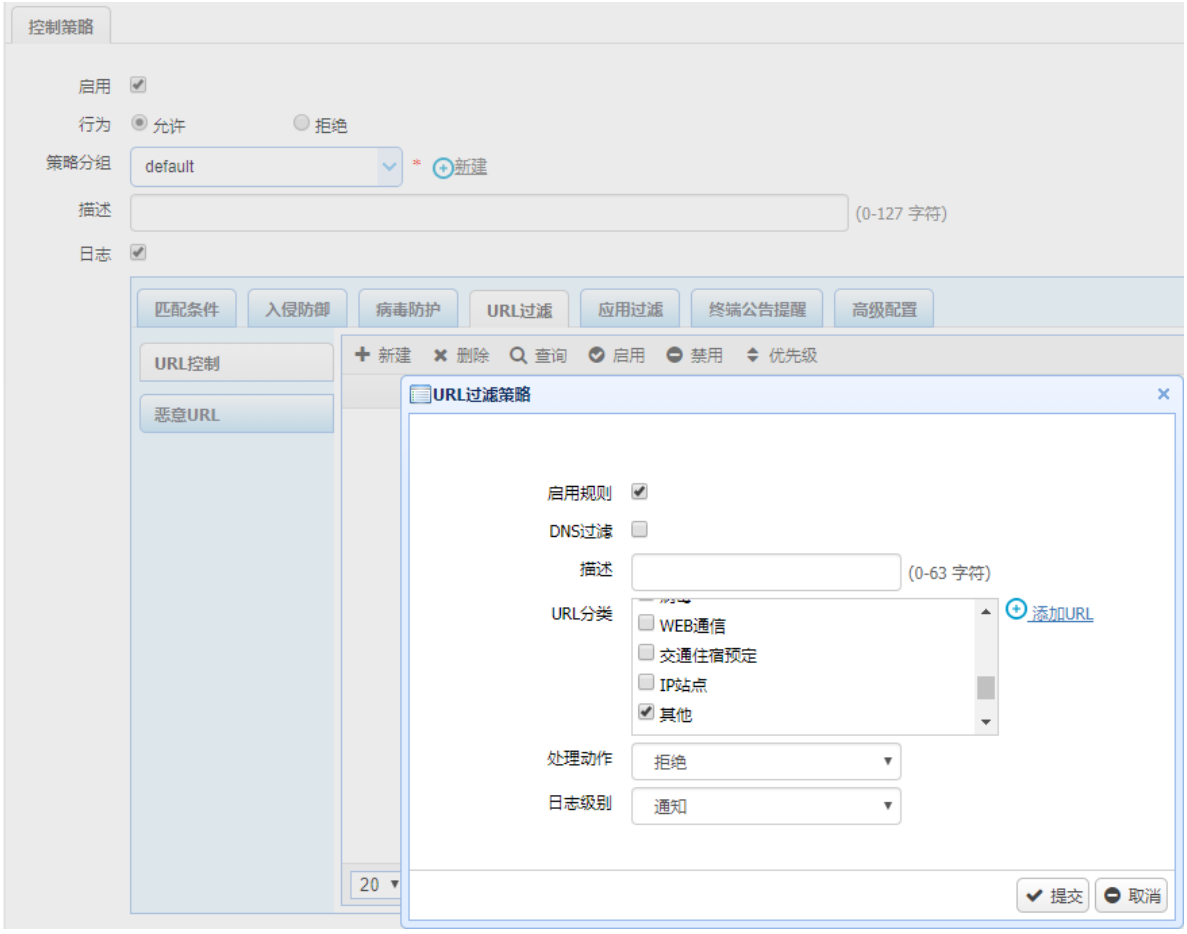
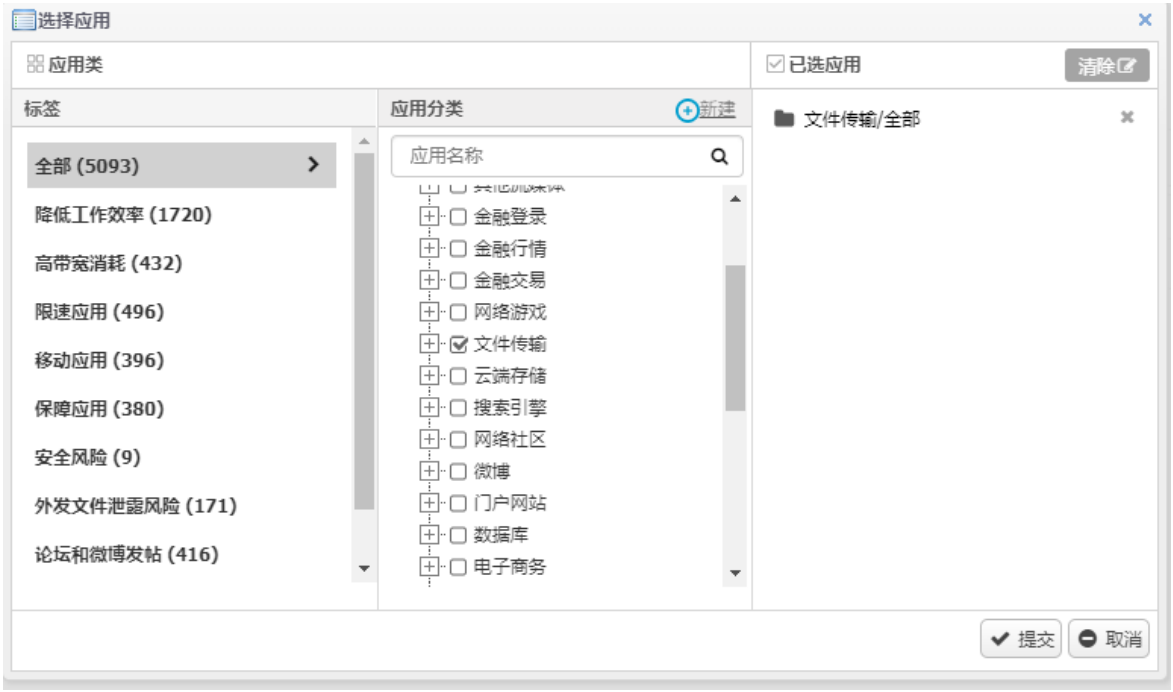


图1-18 URL 控制策略配置完成

(3) 配置应用过滤策略。

单击选择“应用过滤”标签页，新建一条应用过滤策略，应用分类选择“文件传输”，如下图所示。

图1-19 应用过滤策略选择应用



处理动作选择“拒绝”，日志级别配置为“通知”，如下图所示。

图1-20 基于 IPv6 的控制策略-新建应用过滤策略

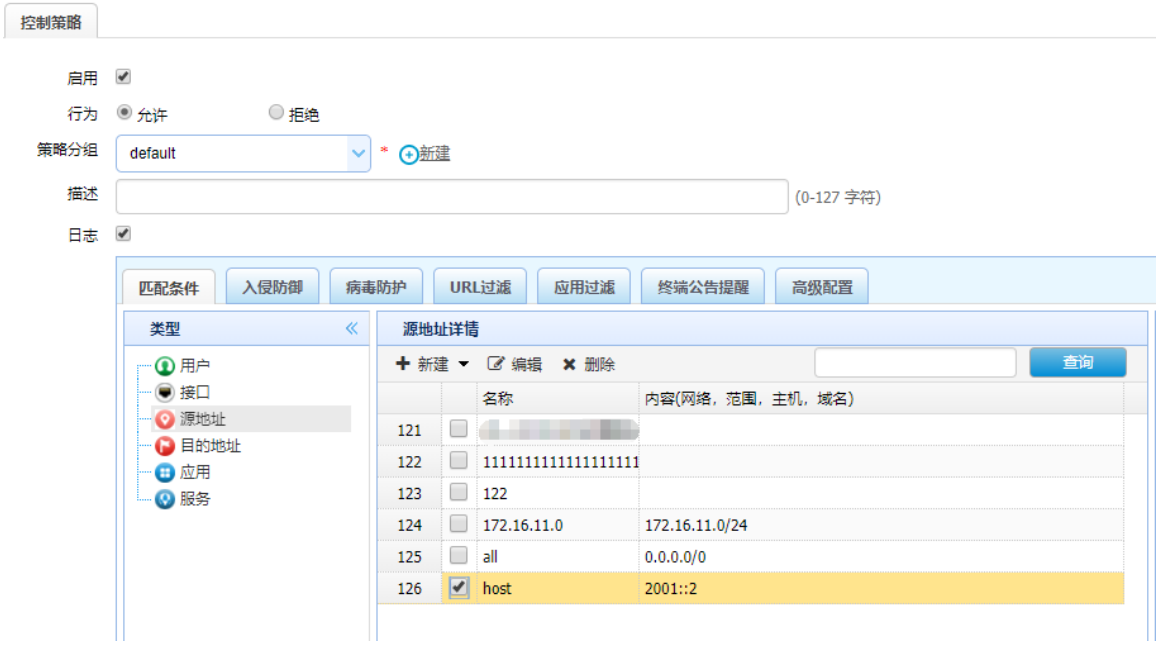
点击<提交>按钮，提交应用过滤配置，如下图所示。

图1-21 应用过滤策略配置完成

(4) 选择源地址为 IPv6 地址对象 host。

单击选择“匹配条件”标签页，源地址选择“host”,，如下图所示。

图1-22 应用过滤策略选择应用



点击 IPv6 策略配置页面的<提交>按钮，完成 IPv6 策略配置。

图1-23 基于 IPv6 的控制策略配置完成

5. 验证配置

配置完成后，内网用户 host 通过 IPv6 地址能 ping 通远端 IPv6 服务器，访问远端服务器 IPv6 的 HTTP 服务和登录 FTP 服务被拒绝。

1.2 WEB关键字过滤

1.2.1 WEB 关键字过滤概述

web 关键字过滤，支持针对搜索引擎内容的过滤、HTTP 上传 POST 内容的过滤以及 HTTP 网页浏览内容的过滤，实现效果如下：

- 搜索引擎：

对搜索引擎的搜索内容进行监控，提供告警、拒绝两种处理动作，并支持记录日志。

- HTTP 上传：

对 http 上传的 POST 内容进行监控，提供告警、拒绝两种处理动作，并支持记录日志，如：

web 邮件过滤（发件人、收件人，主题、内容、附件名）；

web 社区论坛（发帖内容、附件上传）。

- 网页内容：

支持所有 http 网页浏览内容过滤，网页内容必须为文本形式，不能为图片中的文字。

1.2.2 WEB 关键字页面

在导航栏中选择“策略配置 > 控制策略”，单击<新建>按钮，选择“应用过滤 > WEB 关键字”标签页，如图 1-24 所示。

图1-24 WEB 关键字页面

页面上方的快捷功能按钮说明，如表 1-7 所示。

表1-7 快捷功能按钮说明

标题项	说明
新建	点击新建创建规则。
删除	选中对应规则进行快捷删除。

标题项	说明
查询	支持根据条件查询规则。
启用	支持选中对应规则进行快捷启用。
禁用	支持选中对应规则进行快捷禁用。
优先级	支持对选中规则调整优先级顺序。

点击<查询>按钮，可根据条件查询规则，如图 1-25 所示。查询页面详细说明，如表 1-8 所示。

图1-25 查询按钮

表1-8 查询页面详细说明

标题项	说明
ID	根据ID查询WEB关键字规则。
描述	根据描述查询WEB关键字规则。
处理动作	根据处理动作查询WEB关键字规则。
日志级别	根据日志级别查询WEB关键字规则。
重置	清空当前查询页面信息。
提交	提交后根据查询条件显示结果。
取消	取消查询操作。

点击<优先级>按钮，如图 1-26 所示。优先级配置详细说明，如表 1-9 所示。

图1-26 策略优先级配置

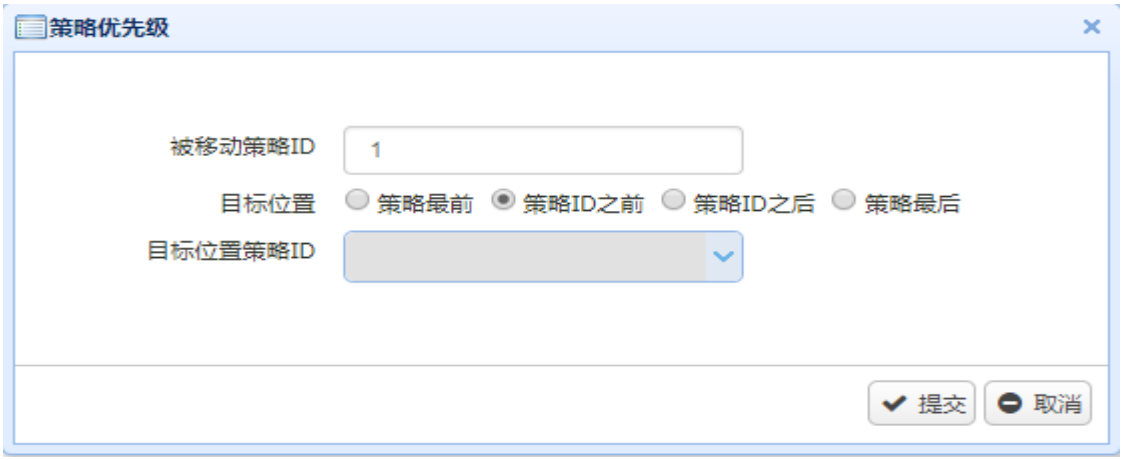


表1-9 策略优先级按钮详细说明

标题项	说明
被移动策略ID	当前操作的策略ID。
目标位置	移动的目标位置，包括：策略最前、策略ID之前、策略ID之后、策略最后。
目标策略ID	选择的目标策略ID，只有目标位置为策略ID之前和策略ID之后时此选项生效。

1.2.3 搜索引擎规则

在导航栏中选择“策略配置 > 控制策略”，单击<新建>按钮，选择“应用过滤>WEB 关键字>搜索引擎”标签页，点击<新建>进入搜索引擎规则配置界面，如图 1-27 所示。搜索引擎规则详细配置说明，如表 1-10 所示。

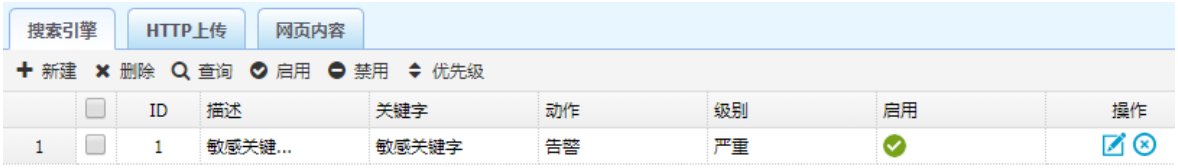
图1-27 搜索引擎规则

表1-10 搜索引擎规则详细配置

标题项	说明
启用	勾选后则启用搜索引擎规则。
描述	搜索引擎规则的描述信息。
关键字对象	选择关键字对象，支持通过<添加关键字>按钮来快速创建关键字对象。
处理动作	处理动作包括：告警、拒绝。
日志级别	日志级别包含：紧急、告警、严重、错误、警告、通知、信息、调试、不记录。
提交	提交后当前规则新建成功。
取消	取消规则创建，不下发配置。

搜索引擎规则创建成功后如图 1-28 所示。

图1-28 搜索引擎规则配置显示



1.2.4 HTTP 上传规则

在导航栏中选择“策略配置 > 控制策略”，单击<新建>按钮，选择“应用过滤>WEB 关键字> HTTP 上传”标签页，点击<新建>进入 HTTP 上传规则配置界面，如图 1-29 所示。HTTP 上传规则详细配置说明，如表 1-11 所示。

图1-29 HTTP 上传规则

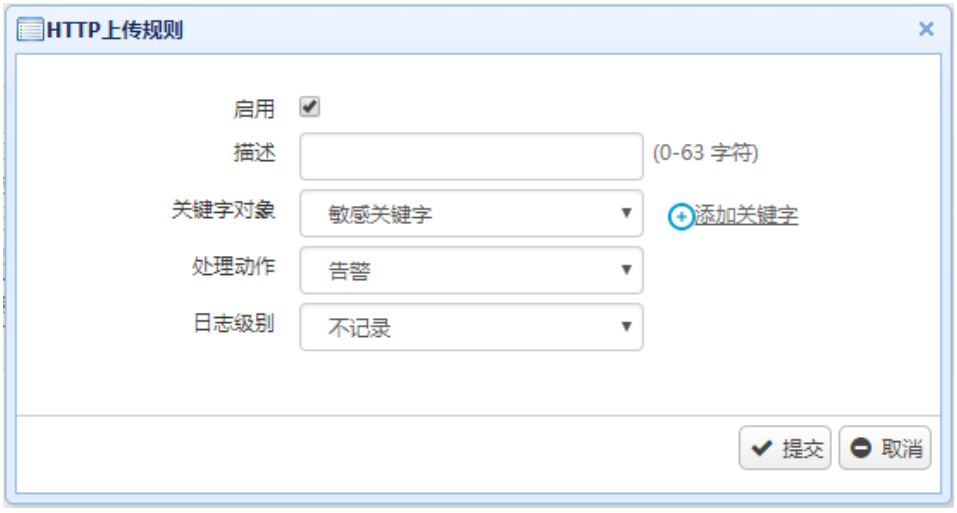


表1-11 HTTP 上传规则详细配置说明

标题项	说明
启用	勾选后则启用搜索引擎规则。
描述	HTTP上传规则的描述信息。
关键字对象	选择关键字对象，支持通过<添加关键字>按钮来快速创建关键字对象。
处理动作	处理动作包括：告警、拒绝。
日志级别	日志级别包含：紧急、告警、严重、错误、警告、通知、信息、调试、不记录。
提交	提交后当前规则新建成功。
取消	取消规则创建，不下发配置。

HTTP 上传规则创建成功后如图 1-30 所示。规则显示详细说明，如表 1-12 所示。

图1-30 HTTP 上传规则配置显示

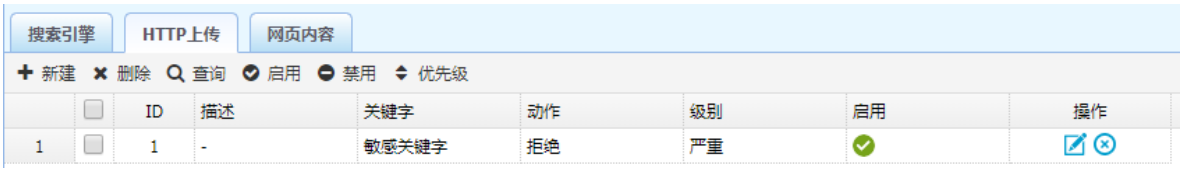


表1-12 HTTP 上传规则显示详细说明

标题项	说明
ID	规则对应ID，代表规则优先级。
描述	规则描述信息显示。
关键字	规则引用的关键字对象。
动作	规则动作，包括：告警、拒绝。
级别	规则日志级别，包括：紧急、告警、严重、错误、警告、通知、信息、调试、不记录。
启用	规则启用状态显示，包括：启用和禁用。
操作	支持对当前规则进行编辑和删除。

1.2.5 网页内容规则

在导航栏中选择“策略配置 > 控制策略”，单击<新建>按钮，选择“应用过滤>WEB 关键字>网页内容”标签页，点击<新建>进入网页内容规则配置界面，如图 1-31 所示。网页内容规则详细配置说明，如表 1-13 所示。

图1-31 网页内容规则

表1-13 网页内容规则详细配置说明

标题项	说明
启用	勾选后则启用搜索引擎规则。
描述	网页内容规则的描述信息。
关键字对象	选择关键字对象，支持通过<添加关键字>按钮来快速创建关键字对象。
处理动作	处理动作包括：告警、拒绝。
日志级别	日志级别包含：紧急、告警、严重、错误、警告、通知、信息、调试、不记录。
提交	提交后当前规则新建成功。
取消	取消规则创建，不下发配置。

网页内容规则创建成功后如图 1-32 所示。规则显示详细说明，如表 1-14 所示。

图1-32 网页内容规则配置显示

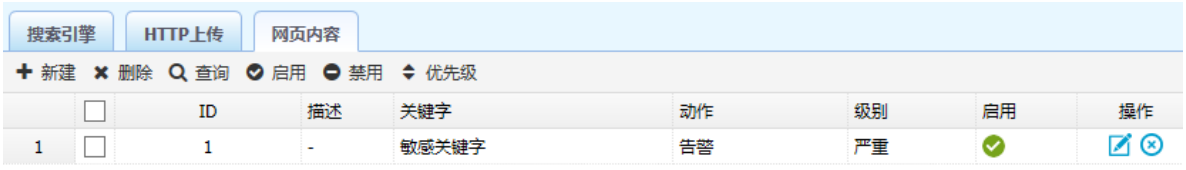


表1-14 网页内容规则配置显示详细说明

标题项	说明
ID	规则对应ID，代表规则优先级。
描述	规则描述信息显示。
关键字	规则引用的关键字对象。
动作	规则动作，包括：告警、拒绝。
级别	规则日志级别，包括：紧急、告警、严重、错误、警告、通知、信息、调试、不记录。
启用	规则启用状态显示，包括：启用和禁用。
操作	支持对当前规则进行编辑和删除。

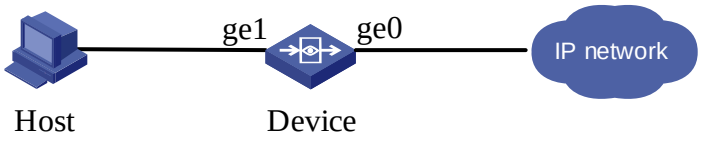
1.2.6 WEB 关键字过滤配置案例

1. 组网需求

针对内网用户上网不允许搜索引擎查找敏感关键字“毒品”，不允许外发 WEB 邮件内容包含敏感关键字“内网资产”，不允许浏览包含关键字“新闻”的网页。

2. 组网图

图1-33 WEB 关键字组网图

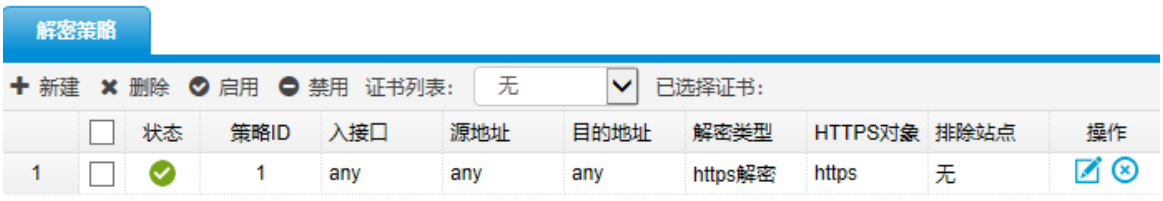


3. 配置步骤

(1) 创建解密策略。

由于部分测试网站为 https 加密网站，需要解密后才能识别到关键字，所以需要先创建解密策略，在导航栏中选择“策略配置 > SSL 解密策略”，单击<新建>按钮，配置完成后下发，如图 1-34 所示。

图1-34 解密策略配置



(2) 创建关键字对象。

在导航栏中选择“策略配置 > 对象管理 > 关键字对象”，单击<新建>按钮，进入关键字对象配置页面，如图 1-35 所示。

图1-35 关键字对象配置

点击<提交>按钮，提交配置。

(3) 创建 WEB 关键字过滤规则

在导航栏中选择“策略配置 > 控制策略”，点击<新建>，在弹出页面中单击选择“应用过滤>WEB 关键字”，分别创建搜索引擎规则、HTTP 上传规则、网页内容规则，如图 1-36、图 1-37、图 1-38 所示。

图1-36 搜索引擎规则

图1-37 HTTP 上传规则

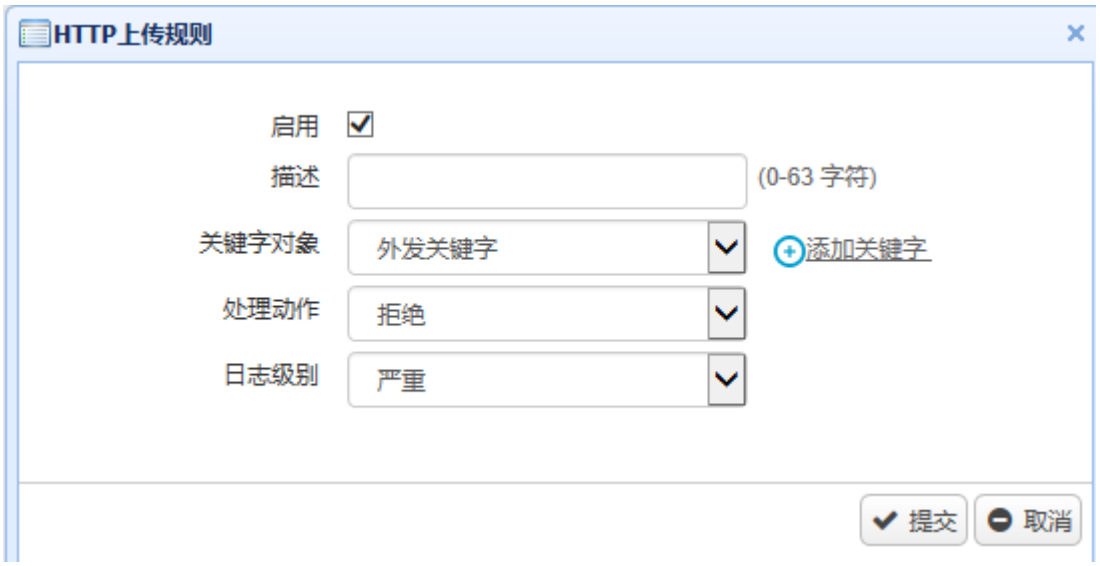


图1-38 网页内容规则

点击<提交>按钮，提交配置。

4. 验证配置

(1) 搜索引擎结果验证

使用百度搜索引擎搜索关键字“毒品”，访问被阻断，无结果回显，同时可以在导航栏“数据中心 > 日志中心 > 控制日志 > 应用控制日志”中产生相应阻断日志，如图 1-39、图 1-40 所示。

图1-39 关键字搜索结果

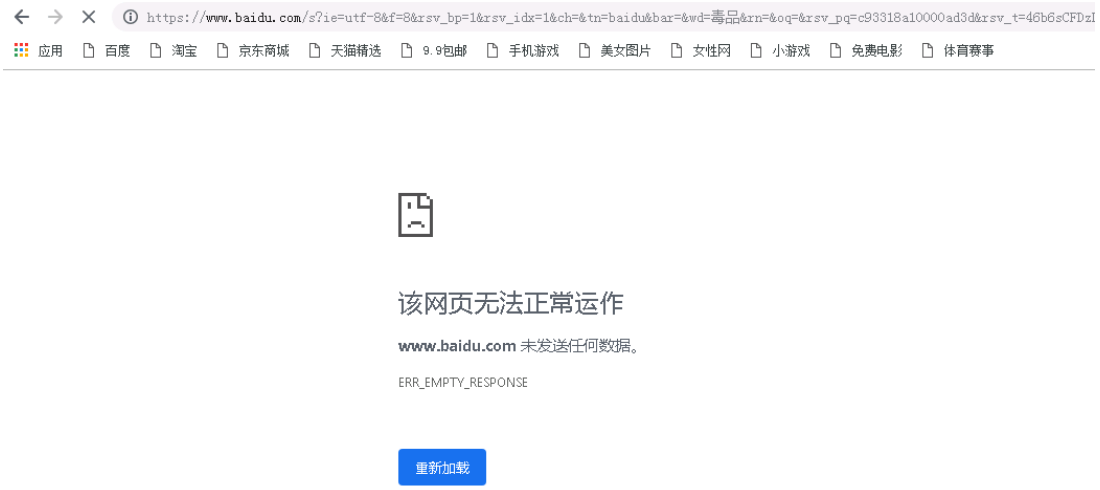
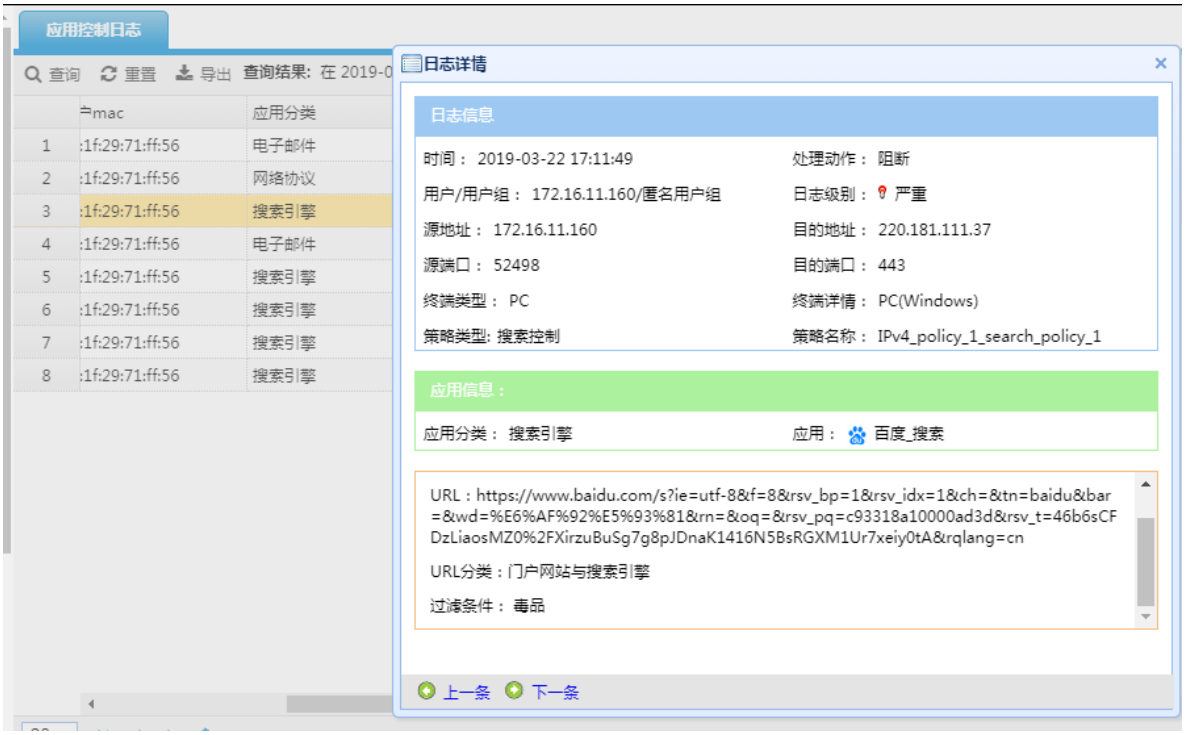


图1-40 应用控制日志

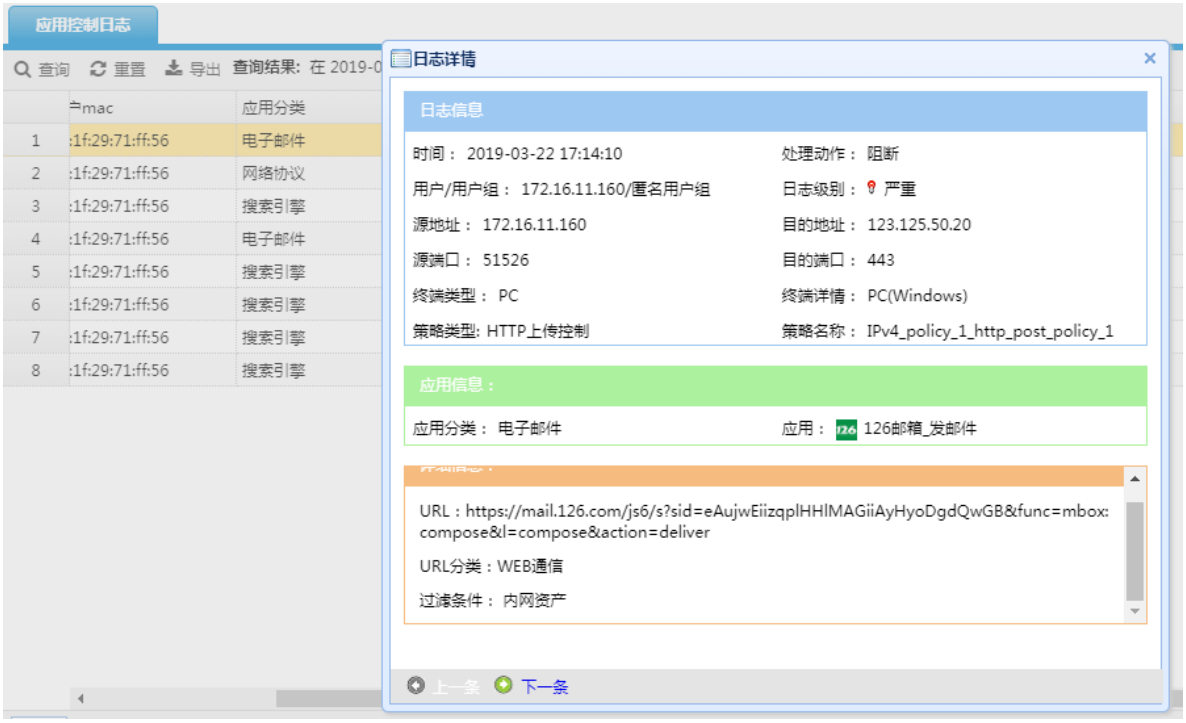


(2) WEB 邮箱结果验证

使用 126 邮箱发送邮件，内容为：内网资产信息请查收，点击发送，邮件无法发送成功，同时可以在导航栏“数据中心 > 日志中心 > 控制日志 > 应用控制日志”中产生相应阻断日志，如图 1-41、图 1-42 所示。

图1-41 邮件发送

图1-42 应用控制日志

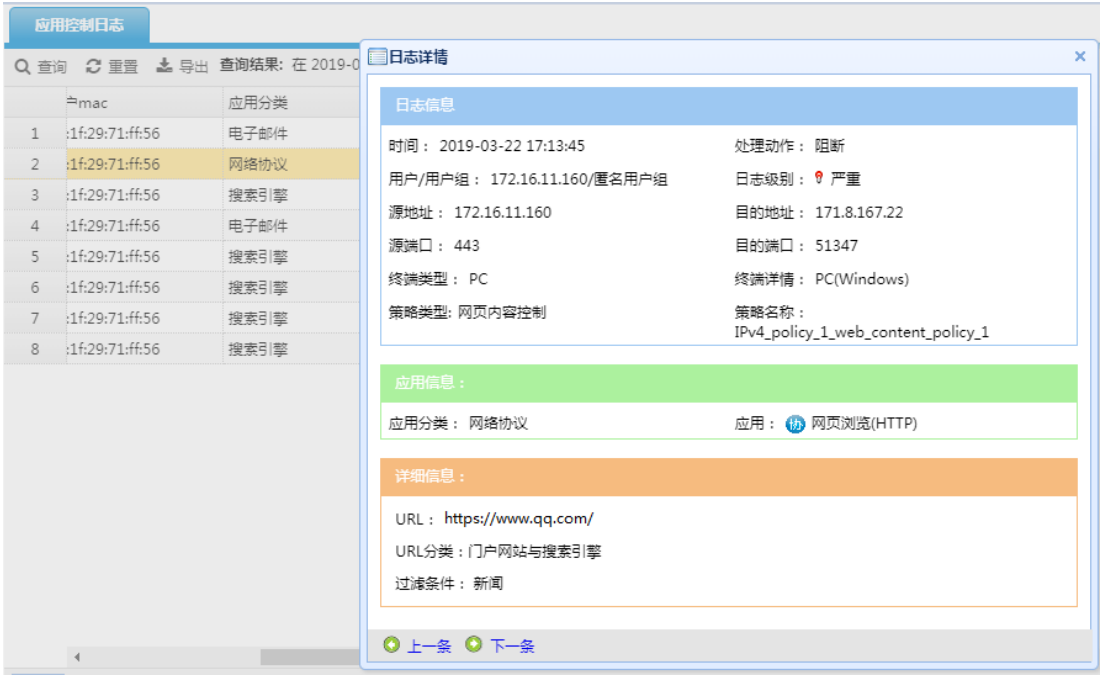


(3) 网页浏览结果验证

使用测试 PC 访问腾讯网站 www.qq.com，同时可以在导航栏“数据中心 > 日志中心 > 控制日志 > 应用控制日志”中产生相应阻断日志，如图 1-43、图 1-44 所示。

图1-43 访问腾讯

图1-44 应用控制日志



1.3 URL过滤

1.3.1 URL 过滤概述

URL 过滤是基于 URL 分类来对用户访问 WEB 站点进行控制，控制动作包含允许和拒绝。这样可以通过对 HTTP 协议的控制为用户提供应用级的安全防护和访问限制。

说明

对 URL 或恶意 URL 进行控制，需要配置解密类型为 HTTPS 解密的 SSL 解密策略，且 HTTPS 对象需包含访问 HTTPS 页面的域名，用户访问 HTTPS 页面被阻断时，才可以弹出阻断提示信息。

1.3.2 URL 过滤策略页面

在导航栏中选择“策略配置 > 控制策略”，单击<新建>按钮，选择“URL 过滤>URL 控制”标签页，新建 URL 过滤策略，如图 1-45 所示。URL 过滤策略页面详细配置说明，如表 1-15 所示。

图1-45 URL 过滤策略

表1-15 URL 过滤策略详细配置

标题项	说明
启用	勾选后则启用URL过滤策略。

标题项	说明
DNS过滤	勾选后则启用DNS过滤功能。启用DNS过滤功能且URL策略配置为阻断时，终端访问域名时，DNS查询请求无法通过设备转发出去，终端无法获得要访问的域名的IP地址。
描述	URL过滤策略的描述信息。
URL分类	URL预定义分类和自定义分类。
处理动作	处理动作包括：允许、拒绝。
日志级别	日志级别包含：紧急、告警、严重、错误、警告、通知、信息、调试、不记录。
提交	提交后当前规则新建成功。
取消	取消规则创建，不下发配置。

URL 过滤策略创建成功后如图 1-46 所示。策略显示详细说明，如表 1-16 所示。

图1-46 URL 过滤策略配置显示

表1-16 URL 过滤策略配置显示详细说明

标题项	说明
ID	策略对应ID，代表策略优先级。
描述	策略描述信息显示。
URL分类	URL预定义分类和自定义分类。
动作	规则动作，包括：允许、拒绝。
级别	规则日志级别，包括：紧急、告警、严重、错误、警告、通知、信息、调试、不记录。
启用	规则启用状态显示，包括：启用和禁用。
操作	支持对当前规则进行编辑和删除。

1.3.3 恶意 URL 页面

在导航栏中选择“策略配置 > 控制策略”，单击<新建>按钮，选择“URL 过滤>恶意 URL”标签页，如图 1-47 所示。恶意 URL 过滤页面详细配置说明，如表 1-17 所示。

图1-47 恶意 URL 页面

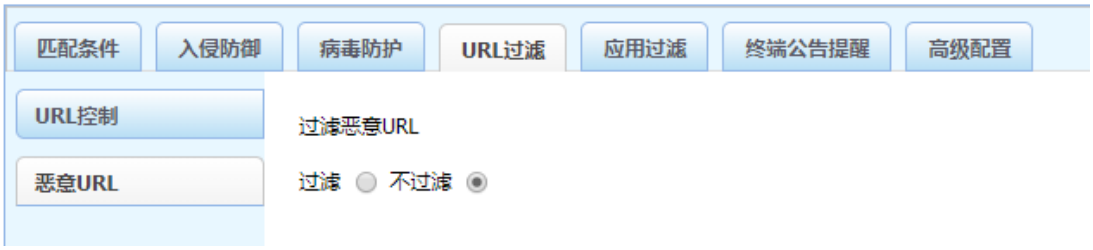


表1-17 恶意 URL 过滤详细配置

标题项	说明
过滤	勾选后则启用恶意URL过滤策略。
不过滤	勾选后则关闭恶意URL过滤策略。

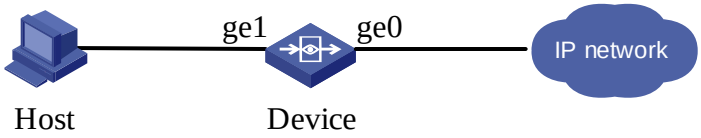
1.3.4 URL 过滤配置案例

1. 组网需求

针对内网用户不允许访问"新闻媒体"网站。

2. 组网图

图1-48 应用控制组网图

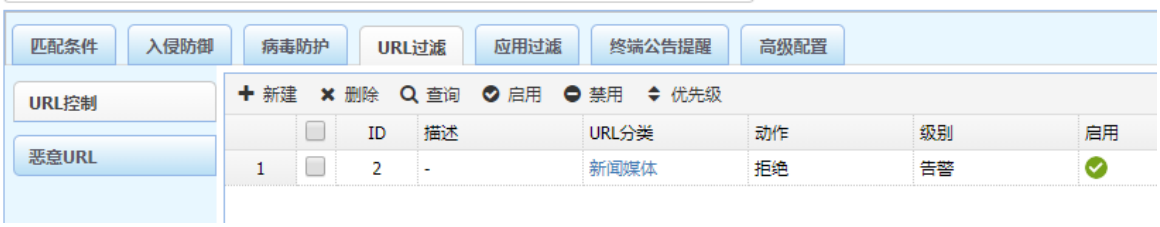


3. 配置步骤

(1) 创建 URL 过滤策略

在导航栏中选择“策略配置 > 控制策略”，点击<新建>，选择“URL 过滤>URL 控制”标签页，创建 URL 过滤策略，如图 1-49 所示。

图1-49 创建 URL 过滤策略



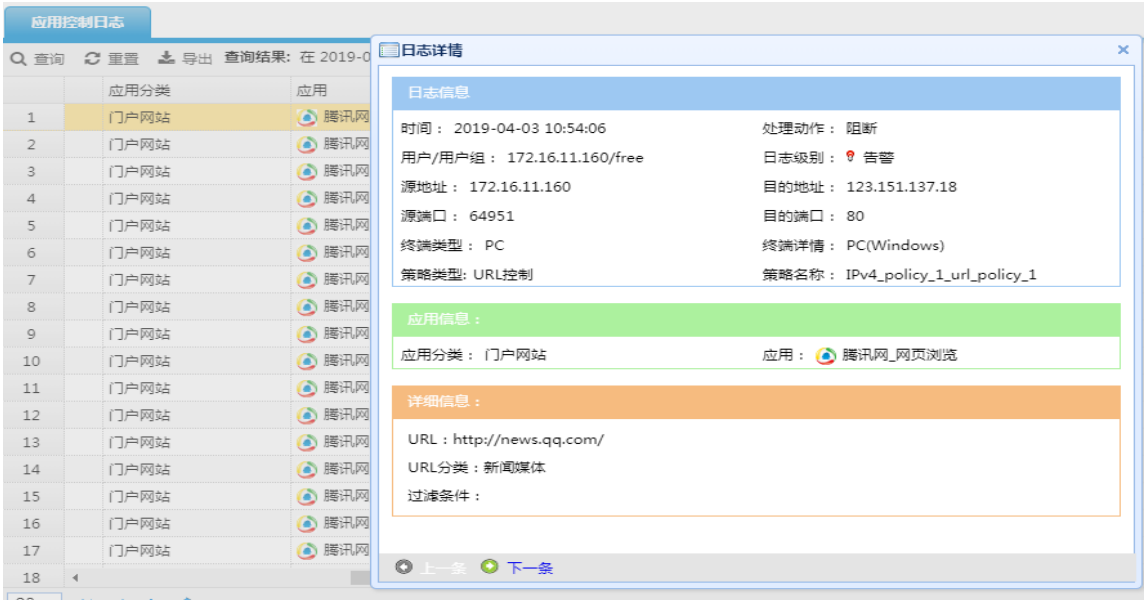
点击<提交>按钮，提交配置。

4. 验证配置

使用终端访问腾讯新闻网站 news.qq.com，访问被阻断，同时可以在导航栏“数据中心 > 日志中心 > 控制日志 >应用控制日志”中产生相应阻断日志，如图 1-50、图 1-51 所示。

图1-50 访问阻断

图1-51 应用控制日志



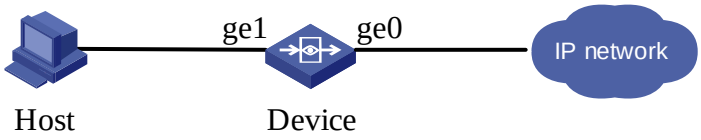
1.3.5 DNS 过滤配置案例

1. 组网需求

针对内网用户不允许获取”新闻媒体”类型的 DNS。

2. 组网图

图1-52 应用控制组网图



3. 配置步骤

(1) 创建 URL 过滤策略

在导航栏中选择“策略配置 > 控制策略”，点击<新建>，选择“URL 过滤>URL 控制”标签页，创建 URL 过滤策略，并且勾选 DNS 过滤，如下图所示。

图1-53 创建 URL 过滤策略

点击<提交>按钮，提交配置。

4. 验证配置

使用终端访问腾讯新闻网站 news.qq.com，因为无法通过 DNS 获取 IP 地址，访问被阻断，同时可以在导航栏“数据中心 > 日志中心 > 控制日志 >应用控制日志”中产生相应阻断日志，如下图所示。

图1-54 访问阻断

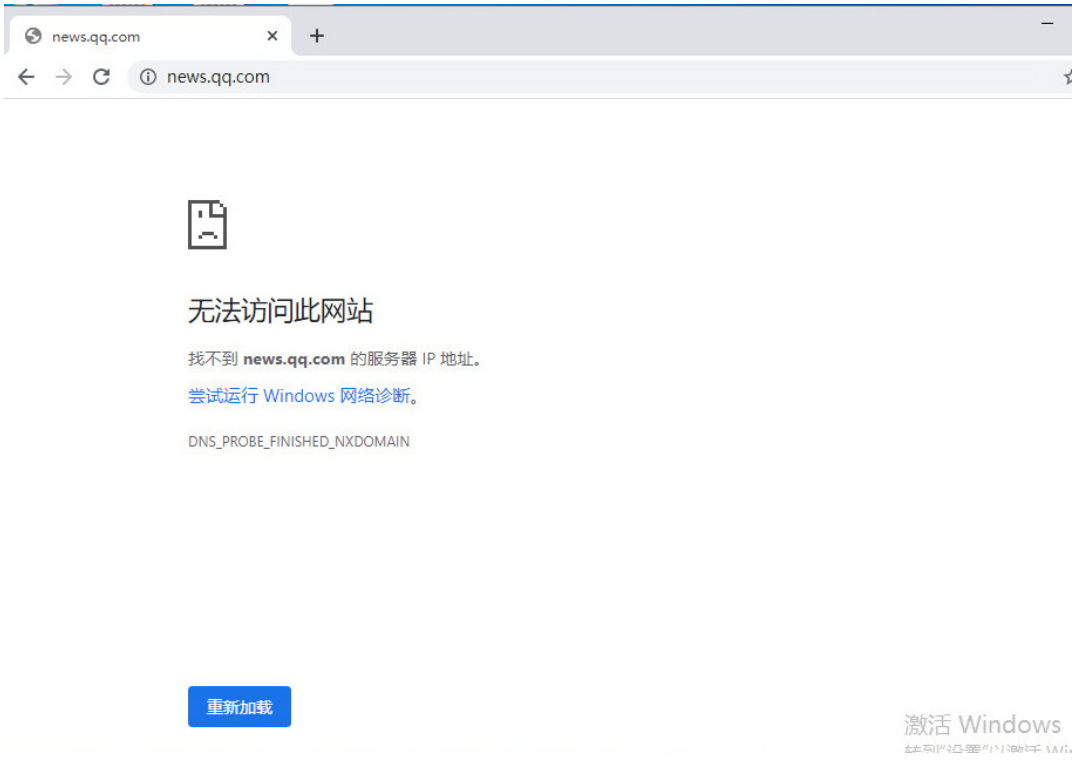
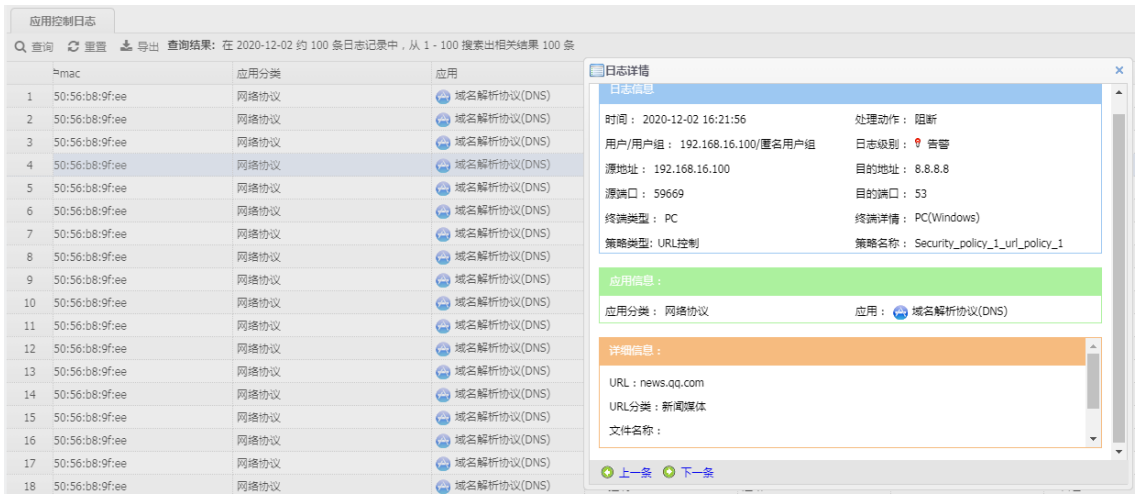


图1-55 应用控制日志



1.4 应用控制

1.4.1 应用控制概述

应用控制是基于应用对象来进行控制，控制动作包含允许和拒绝。

1.4.2 应用控制页面

在导航栏中选择“策略配置 > 控制策略”，单击<新建>，选择“应用过滤>应用控制”标签页，新建应用控制策略，如图 1-56 所示。应用控制页面详细配置说明，如表 1-18 所示。

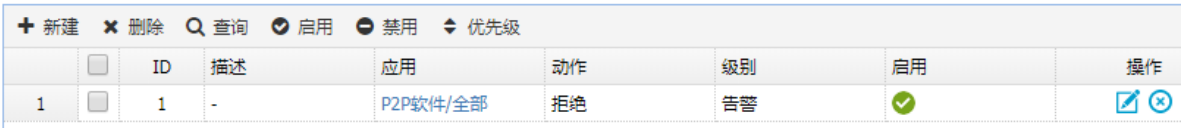
图1-56 应用控制

表1-18 应用控制详细配置

标题项	说明
启用	勾选后则启用搜索引擎规则。
描述	搜索引擎规则的描述信息。
应用	应用对象，通过点击<选择应用>弹框来选择相关的应用。
处理动作	处理动作包括：告警、拒绝。
日志级别	日志级别包含：紧急、告警、严重、错误、警告、通知、信息、调试、不记录。
提交	提交后当前规则新建成功。
取消	取消规则创建，不下发配置。

应用控制策略创建成功后如图 1-57 所示。

图1-57 应用控制配置显示



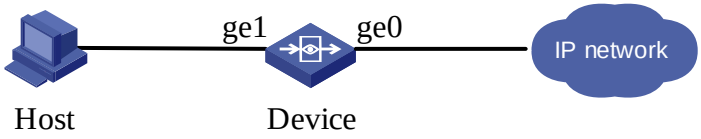
1.4.3 应用控制配置案例

1. 组网需求

针对内网用户不允许玩游戏，将所有游戏应用全部阻断。

2. 组网图

图1-58 应用控制组网图



3. 配置步骤

(1) 创建应用控制策略

在导航栏中选择“策略配置 > 控制策略”，点击<新建>，在弹出页面中选择“应用过滤>、<应用控制”标签页，创建应用控制策略，如图 1-59 所示。

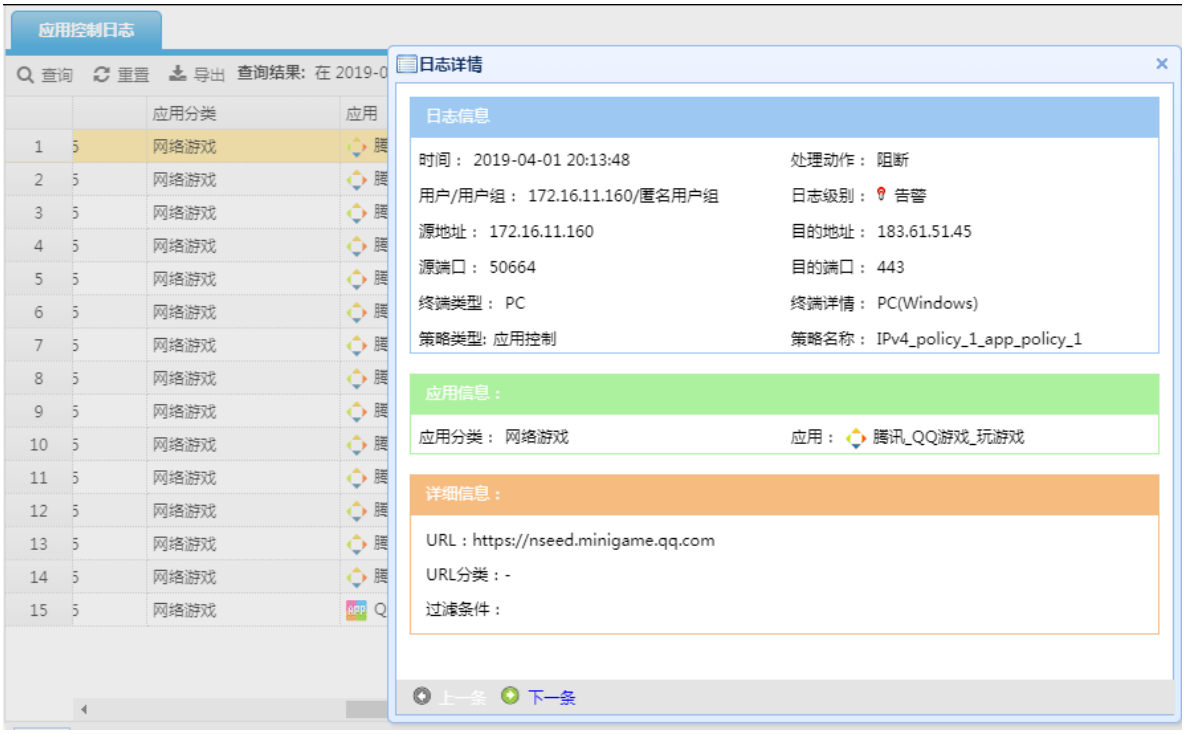
图1-59 创建应用控制策略

点击<提交>按钮，提交配置。

4. 验证配置

使用终端登录腾讯 QQ 游戏，无法登录，被阻断，可以在导航栏“数据中心 > 日志中心 > 控制日志 > 应用控制日志”中产生相应阻断日志，如图 1-60 所示。

图1-60 应用控制日志


应用控制日志
查询
重置
导出
查询结果: 在 2019-0
应用分类
应用
网络游戏
日志详情
日志信息
时间： 2019-04-01 20:13:48
处理动作： 阻断
用户/用户组： 172.16.11.160/匿名用户组
日志级别： 告警
源地址： 172.16.11.160
目的地址： 183.61.51.45
源端口： 50664
目的端口： 443
终端类型： PC
终端详情： PC(Windows)
策略类型: 应用控制
策略名称： IPv4_policy_1_app_policy_1
应用信息：
应用分类： 网络游戏
应用： 腾讯_QQ游戏_玩游戏
详细信息：
URL：https://nseed.minigame.qq.com
URL分类：-
过滤条件：
上一条
下一条

1.5 邮件控制

1.5.1 概述

邮件控制策略页面包含发件人过滤、收件人过滤、标题及内容过滤、邮件大小以及附件个数过滤。发件人和收件人过滤包括功能开启、策略属性（黑白名单）以及关键字配置。标题及内容支持关键字配置。

1.5.2 邮件控制

在导航栏中选择“策略配置 > 控制策略”，单击<新建>，选择“应用过滤>邮件控制”标签页，进入如图 1-61 所示页面。在该页面上，可以查看已经配置的邮件控制信息。这些信息的详细说明如表 1-19 所示。

图1-61 邮件控制

表1-19 邮件控制的显示信息

标题项	说明
启用	开启邮件控制功能
发件人过滤-黑名单	黑名单的用户发送邮件会被阻断
发件人过滤-白名单	仅允许白名单的用户发送邮件
收件人过滤-黑名单	黑名单的用户收邮件会被阻断
收件人过滤-白名单	仅允许白名单的用户收邮件

标题项	说明
标题和内容关键字	标题和内容中带有配置的关键字的将会被阻断
邮件大小	发送邮件的大小，如果超过配置值将会被阻断
附件个数	发送附件个数如果大于配置值将会被阻断
日志	邮件被阻断会发送阻断日志，阻断级别可以选择

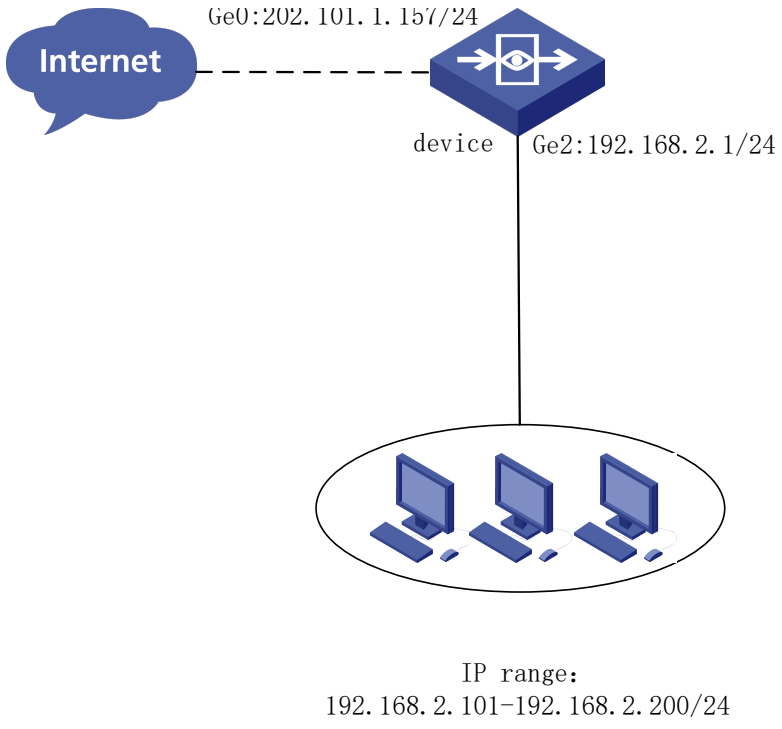
1.5.3 邮件控制配置举例

1. 组网需求

用户 test 发送邮件大小超过 5M，发送的邮件被阻断。

2. 组网图

图1-62 邮件控制组网图



3. 配置步骤

(1) 创建用户 test

进入“用户管理 > 用户组织结构”，新建“test”用户，如图 1-63 所示。

图1-63 用户配置

(2) 配置控制策略

进入“策略配置 > 控制策略”，在“匹配条件”页面，选择用户“test”，并点击<提交>。如图 1-64 所示。

图1-64 配置控制策略

(3) 配置邮件控制策略

在“控制策略配置”页面，选择“应用过滤 > 邮件控制”，配置邮件控制，邮件大小设置为 5M，并点击<提交>按钮提交该页配置，如图 1-65 所示。

图1-65 配置邮件控制

(4) 配置认证策略

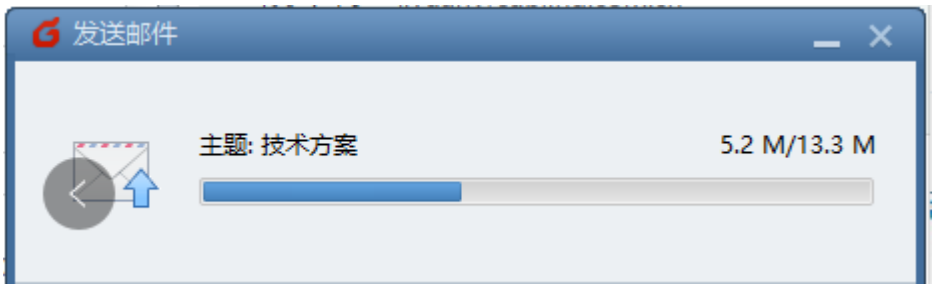
进入“用户管理 > 认证管理 > 认证策略”，配置本地 WEB 认证策略，如图 5-6 所示。

图1-66　　配置本地 WEB 认证

4. 验证配置

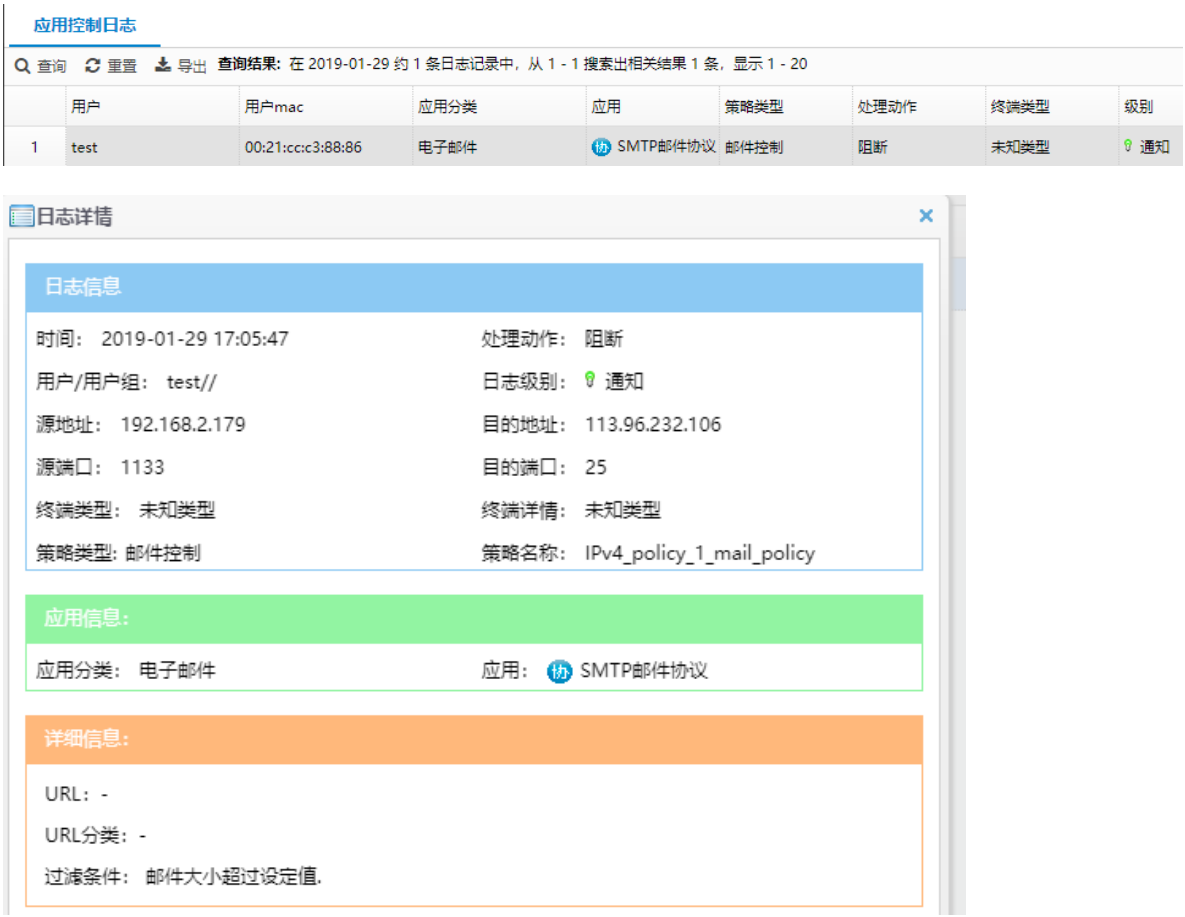
(1)　用户 test 通过本地认证后过设备发送大于 5M 的邮件，邮件发送失败，如图 1-67 所示。

图1-67 邮件发送



(2)　设备应用控制记录阻断日志，可以查看详情，如图 1-68 所示。

图1-68 应用控制记录阻断日志



1.6 虚拟账号

1.6.1 概述

QQ 虚拟账号控制是指控制策略根据所引用关键字对象设置待过滤账号，只允许引用单个关键字对象，关键字过滤只支持精确匹配。根据匹配到的动作（黑名单或白名单）进行 QQ 账号控制并产生应用控制日志。

1.6.2 配置虚拟账号

在导航栏中选择“策略配置 > 控制策略”，单击<新建>，选择“应用过滤>虚拟账号”标签页，进入如图 1-69 所示页面。在该页面上可以配置虚拟账号功能。各个配置项含义如表 1-20 所示。

图1-69 虚拟账号配置页面

表1-20 虚拟账号配置项含义表

标题项	说明
启用	启用虚拟账号功能，未启用状态下无法配置黑白名单。
黑名单	启用虚拟账号黑名单，引用关键字对象，可以直接点击添加关键字按钮添加关键字对象。
白名单	启用虚拟账号白名单，引用关键字对象，可以直接点击添加关键字按钮添加关键字对象。
日志级别	选择匹配到虚拟账号后产生的虚拟账号控制日志级别。

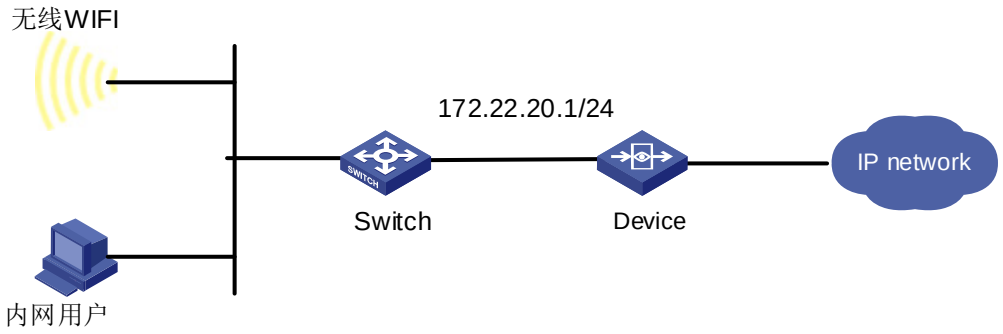
1.6.3 虚拟账号配置举例

1. 组网需求

如图 1-70 所示，公司内网存在内网用户供内部人员使用；无线 WIFI 供访客使用，具体需求如下：

- 针对内网用户，公司内部人员只放行特定的 QQ 账户上网，其它 qq 号阻断登录。
- 针对无线 WIFI 网络，阻断特定 qq 账户，其它 qq 放行可以上网。

图1-70 虚拟账号组网图



2. 配置步骤

(1) 配置地址对象

通过菜单“策略配置 > 对象管理 > 地址对象”，点击<新建>地址对象，配置“内网用户”地址对象和“无线 wifi”地址对象。如图 1-71、图 1-72 所示。

图1-71 添加内网用户地址对象

图1-72 添加无线 wifi 地址对象

(2) 配置关键字对象

通过菜单“策略配置 > 对象管理 > 关键字对象”，点击<新建>关键字对象，配置“QQ 白名单”关键字对象和“QQ 黑名单”关键字对象，如图 1-73、图 1-74 所示。

图1-73 添加 QQ 白名单对象

图1-74 添加 QQ 黑名单对象

(3) 配置控制策略，虚拟账户配置白名单。

通过菜单“策略配置>控制策略”，点击<新建>进入控制策略配置页面，源地址对象选择“内网用户”，虚拟账户启用白名单，如图 1-75、图 1-76 所示。

图1-75 控制策略配置内网用户源地址

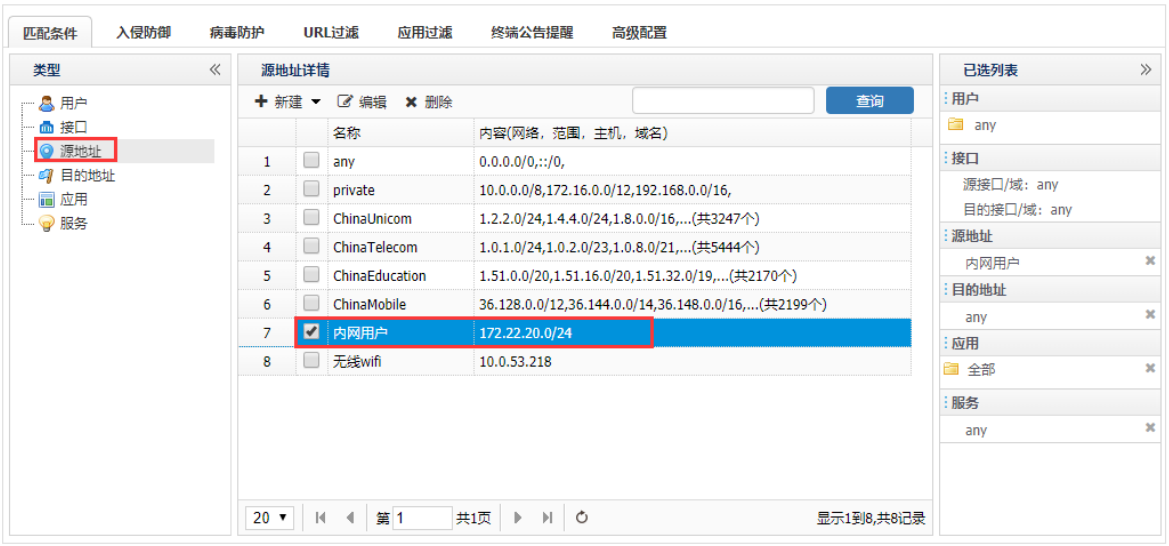


图1-76 控制策略配置虚拟账户白名单控制

(4) 配置控制策略，虚拟账户配置黑名单。

通过菜单“策略配置 > 控制策略”，点击<新建>进入控制策略配置页面，源地址对象选择 “无线wifi”，虚拟账户启用黑名单，如图 1-77、图 1-78 所示。

图1-77 控制策略配置无线 wifi 源地址

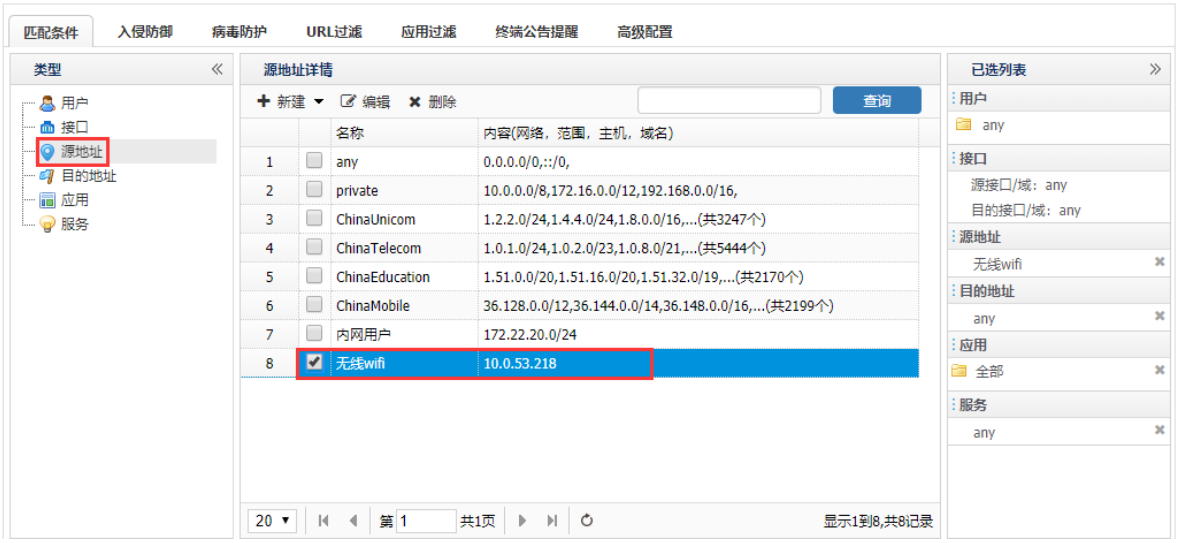


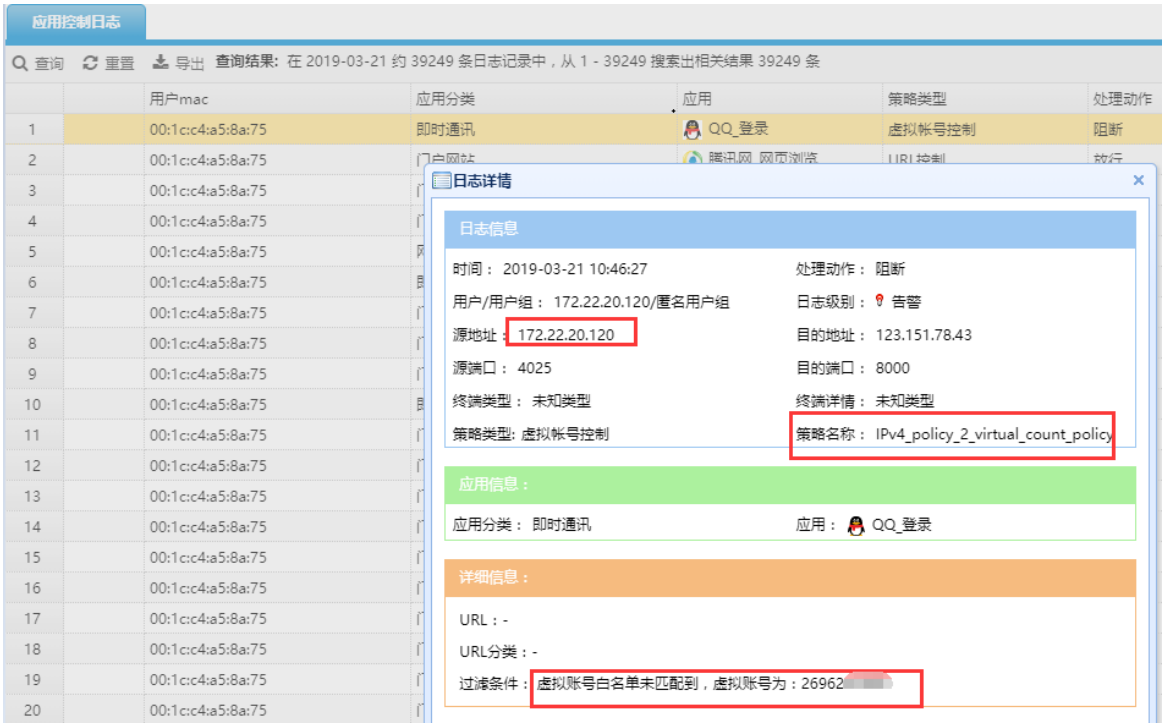
图1-78 控制策略配置虚拟账户黑名单控制

3. 验证结果

(1) 内网用户匹配白名单策略效果

通过菜单“数据中心 > 日志中心 > 控制日志 > 应用控制日志”，查看虚拟控制日志。内网用户使用白名单关键字内的 QQ 账户可以登录，不记录控制日志。使用白名单以外的 QQ 账户，登录账户阻断后，点击日志详情可以查看匹配的策略名称和阻断账户，如图 1-79 所示。

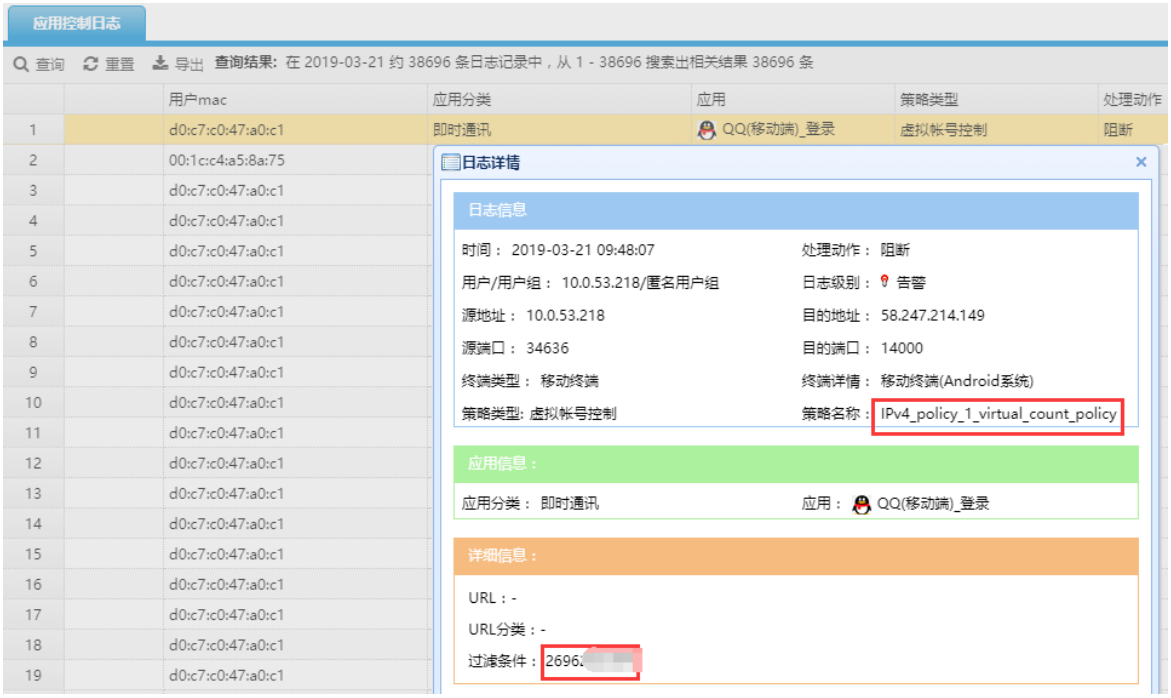
图1-79 内网用户匹配白名单日志



(2) 无线 WIFI 网段用户匹配黑名单策略效果

通过菜单“数据中心 > 日志中心 > 控制日志 > 应用控制日志”，查看虚拟控制日志。无线 WIFI 网段用户使用黑名单以外的关键字登录 qq，可以登录不记录控制日志。使用黑名单关键字的账户登录 qq 阻断后查看控制日志，点击日志条目详细可以看到匹配的策略名称和阻断账户进入如图 1-80 所示的页面。

图1-80 无线 WIFI 用户匹配黑名单日志



1.7 文件类型过滤

1.7.1 文件类型过滤简介

利用网络来进行文件传输是许多用户的重要途径之一，而在文件传输过程中存在种种管理和安全隐患，如用户有意泄密者甚至会将外发文件的后缀名修改，然后通过 HTTP、FTP 协议进行外发则会产生文件的泄漏等安全风险。

支持基于文件类型的过滤行为，封堵 HTTP、FTP 协议传输文件。基于特征能够识别真实的文件类型，即便存在修改、删除外发文件后缀名，也能发现并且告警，保护组织的信息资产安全。

1.7.2 文件类型过滤使用限制

(1) 文件后缀超过 15 个字符时，日志记录会截断前 15 个字符；

(2) 阻断 FTP 时，本地会创建临时的文件；

(3) 升级特征库，预定义文件类型需要手动点击重置才可以更新；

(4) 真实文件类型识别中：jpg 和 jpeg 无法区分；

(5) 开启真实文件类型过滤后，如果识别到真实文件类型为 png，但配置为 jpg 阻断，文件名称后缀为.jpg，不会实现阻断，开启真实文件类型识别后优先进行真实文件判断；

(6) 默认真实文件类型识别为关闭状态；

(7) 解密后真实文件类型应用支持： 163 邮箱（上传/下载）、QQ 邮箱下载、126 邮箱（上传/下载）、百度网盘下载、360 云盘非真实文件类型上传和真实文件类型下载；

(8) 真实文件识别支持类型包括：avi、mp4、mp3、chm、jpg、jpeg、gif、bmp、tiff、png、dcm、heic、ico、jxr、psd、 zip、rar、gz、7z、docx、pptx、xlsx、pdf、rtf。

(9) 文件类型对象匹配不区分大小写，配置 ZIP 与配置 zip 阻断效果一样。

(10) 如果使用的 FTP 连接端口为非标准端口，需要在设备中配置 FTP 非标准端口，配置后就可以正常控制了，HTTP 均是正常可以控制的。

1.7.3 文件类型过滤页面

在导航栏中选择“策略配置 > 控制策略”，单击<新建>，选择“应用过滤>文件类型过滤”标签页，进入如图 1-56 所示页面。在该页面上，点击<新建>进入文件类型过滤配置界面，如下图所示。

图1-81 文件类型过滤页面

图1-82 新建文件类型过滤配置页面

表1-21 文件类型过滤详细配置

标题项	说明
启用	勾选后则启用该文件类型过滤策略。
描述	文件类型过滤策略的描述信息。
文件类型分类	选择文件类型对象，支持通过<添加文件类型>按钮来快速创建文件类型对象。
传输方向	传输方向包括：上传、下载，分别表示HTTP和FTP的上传和下载。
排除网站	仅对http上传下载有效，可以选择URL分类对象进行排除该网站不进行控制。
处理动作	处理动作包括：允许、拒绝。
日志级别	日志级别包含：紧急、告警、严重、错误、警告、通知、信息、调试、不记录。

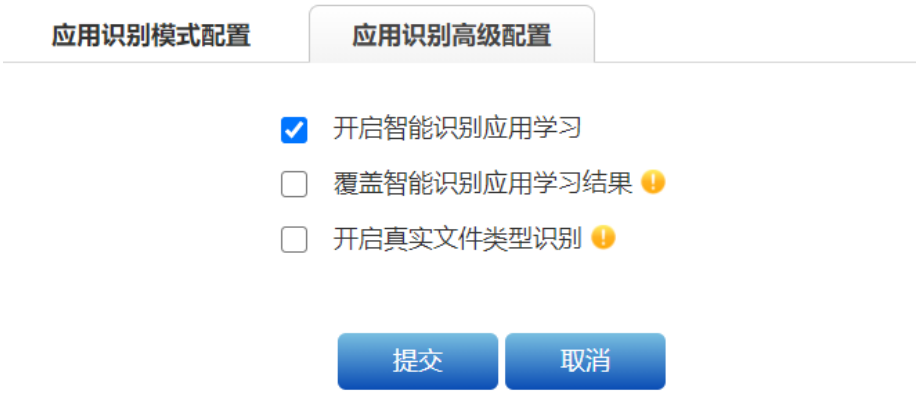
标题项	说明
提交	提交后当前规则新建成功。
取消	取消规则创建，不下发配置。

文件类型过滤策略创建成功后如下图所示。

图1-83 文件类型过滤配置显示

在导航栏中选择“策略配置 > 对象管理 > 应用识别模式”，单击<应用识别高级配置>页签，可以跳转到<应用识别高级审计>页面，在该页面选择是否开启真实文件类型识别选择，如下图所示。

图1-84 开启真是文件类型识别配置显示



说明

- 真实文件识别支持类型如下：avi、mp4、mp3、chm、jpg、jpeg、gif、bmp、tiff、png、dcm、heic、ico、jxr、psd、 zip、rar、gz、7z、docx、pptx、xlsx、pdf、rtf。
- 开启真实文件类型识别后，下载/上传该文件在支持类型列表中就会识别其真实文件类型，即使修改该文件的后缀名，也会只识别其真实的文件类型。

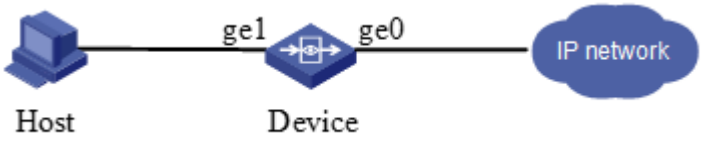
1.7.4 文件类型过滤配置举例

1. 组网需求

针对通过 FTP 或者 HTTP 下载图片文件（JPG）的用户进行阻断。

2. 组网图

图1-85 文件类型过滤测试组网图



3. 配置步骤

在导航栏中选择“策略配置 > 控制策略”，单击<新建>，选择“应用过滤>文件类型过滤”标签页，点击<新建>按钮， 创建文件类型过滤策略，如下图所示。

图1-86 创建文件类型过滤策略

点击<提交>按钮，提交配置。

4. 验证配置

使用测试 PC 过设备通过 HTTP 或者 FTP 下载 png 图片文件，无法下载，被阻断，可以在导航栏“数据中心 > 日志中心 > 控制日志 > 应用控制日志”中产生相应阻断日志，如下图所示。

图1-87 应用控制日志

1.8 终端公告推送

1.8.1 终端公告推送简介

随着网络化的普及，网络的管理也日趋精细，经常需要在网络内部发布公告或通知内容。网络内部可以选择使用终端公告提醒的公告功能，公告发布后，内网终端能够在访问网页时重定向到公告页面，以达到公告的目的。

1.8.2 终端公告推送页面

通过菜单“策略配置>控制策略”，新建一条控制策略，编辑此控制策略，进入如图 1-88 所示页面。在该页面上可以配置终端公告推送的相关功能。各个配置项含义如表 1-22 所示。

图1-88 终端公告推送配置页面

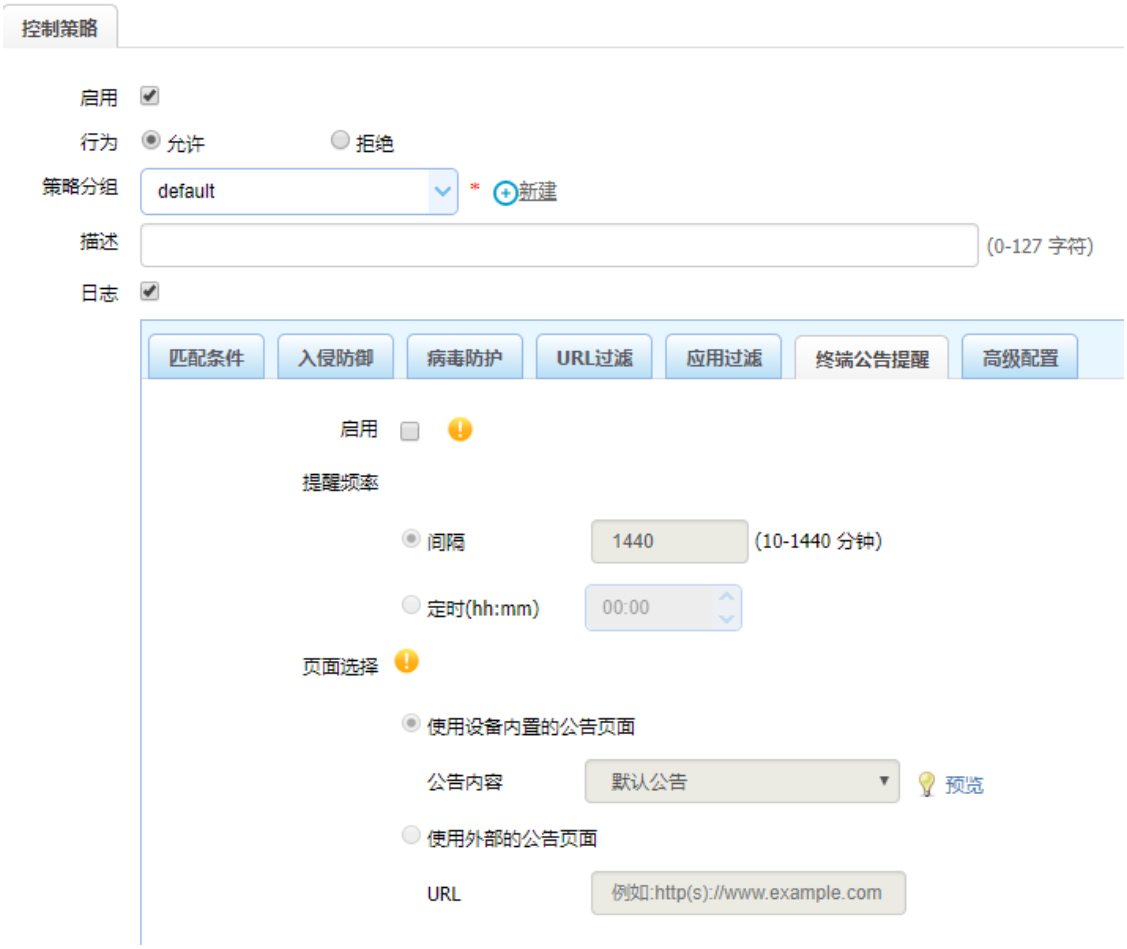


表1-22 终端公告推送配置项含义表

标题项	说明
启用	勾选复选框表示开启终端公告推送功能。
提醒频率（间隔）	按配置间隔阈值，周期性进行公告提醒。

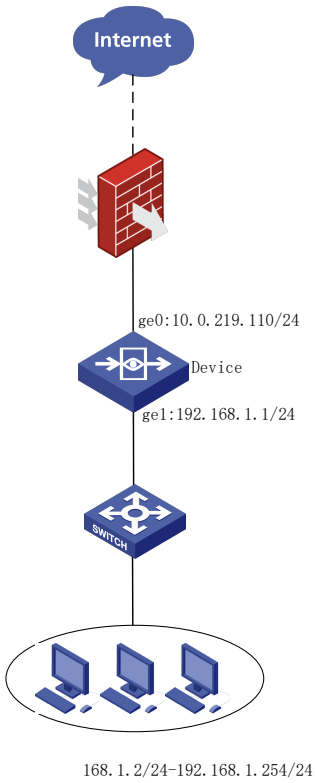
标题项	说明
提醒频率（定时）	配置定时时间，定时进行公告提醒。
页面选择	复选框，可以选择设备内置公告，也可以选择外置公告页面。

1.8.3 终端公告配置举例

1. 组网需求

如图 1-89 所示，某公司为了加强上网管理，拟定了一个上网准则公告，需要周期性进行网络内部推送，使用设备的 ge0 和 ge1 接口以三层路由模式部署在网络中，上联出口 FW，下联二层交换机。设备上开启移动终端公告推送功能，检测上网行为并周期推送公告提醒。

图1-89 终端公告推送组网



2. 配置思路

- 配置设备接口地址及路由。
- 配置地址对象。
- 配置用户识别范围。
- 配置自定义公告内容。
- 开启移动终端公告推送功能。

3. 配置步骤

(1)　配置接口地址

如图 1-90、图 1-91 所示，进入“网络配置 > 接口配置”页面，点击编辑 ge0、ge1 操作，把 ge0、ge1 的地址分别配置为 10.0.219.110/24、192.168.1.1/24。

图1-90 配置 ge0 接口

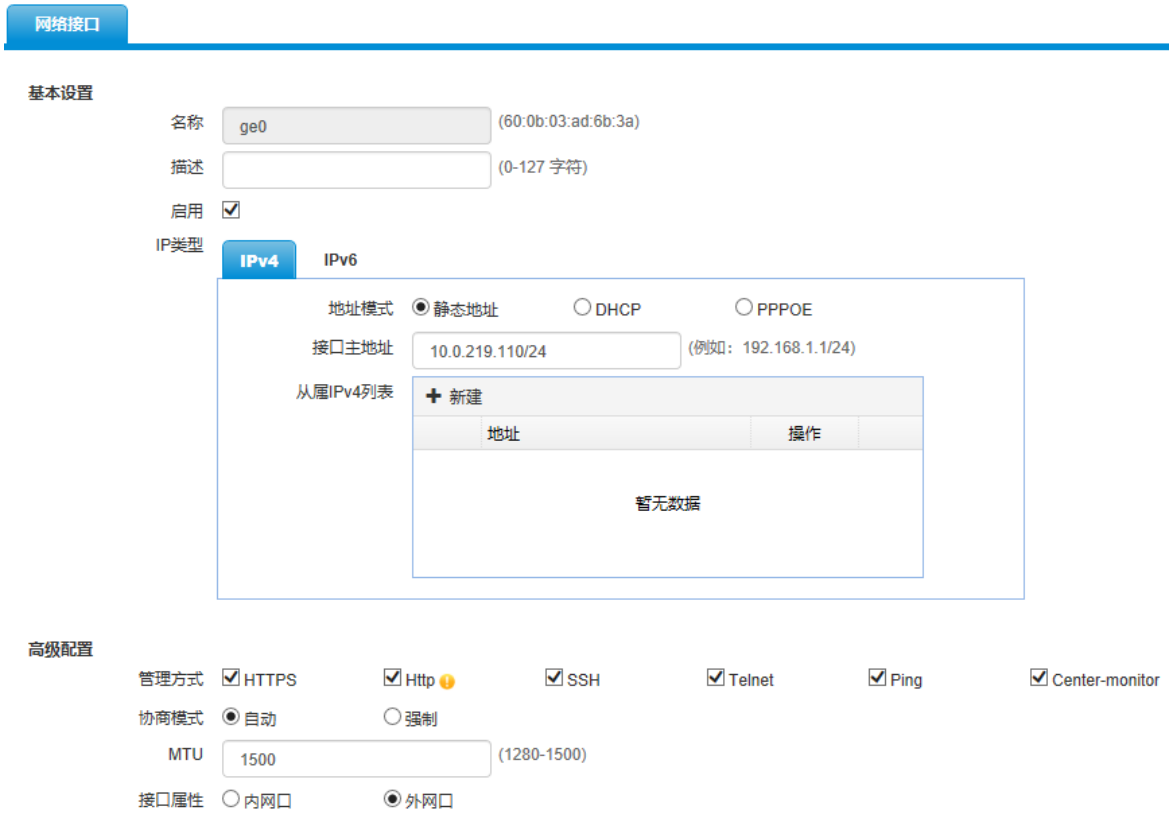
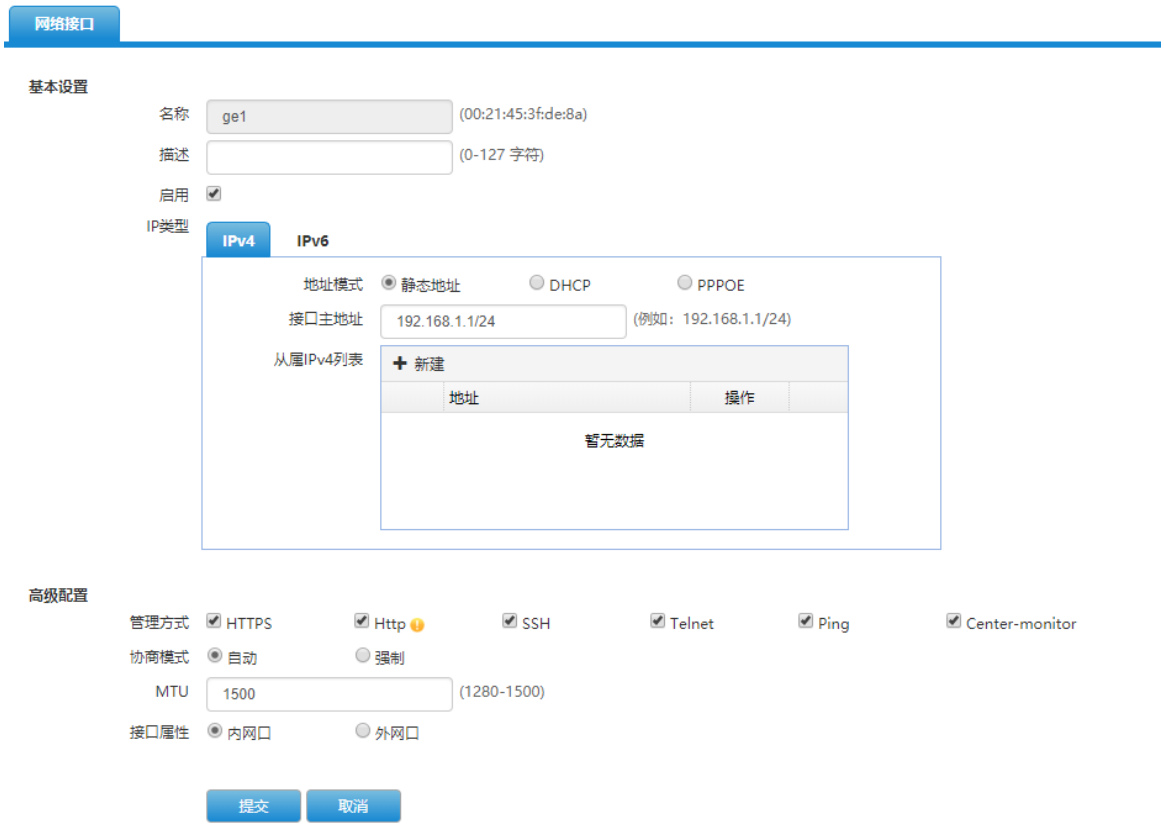


图1-91 配置 ge1 接口



(2) 配置静态路由

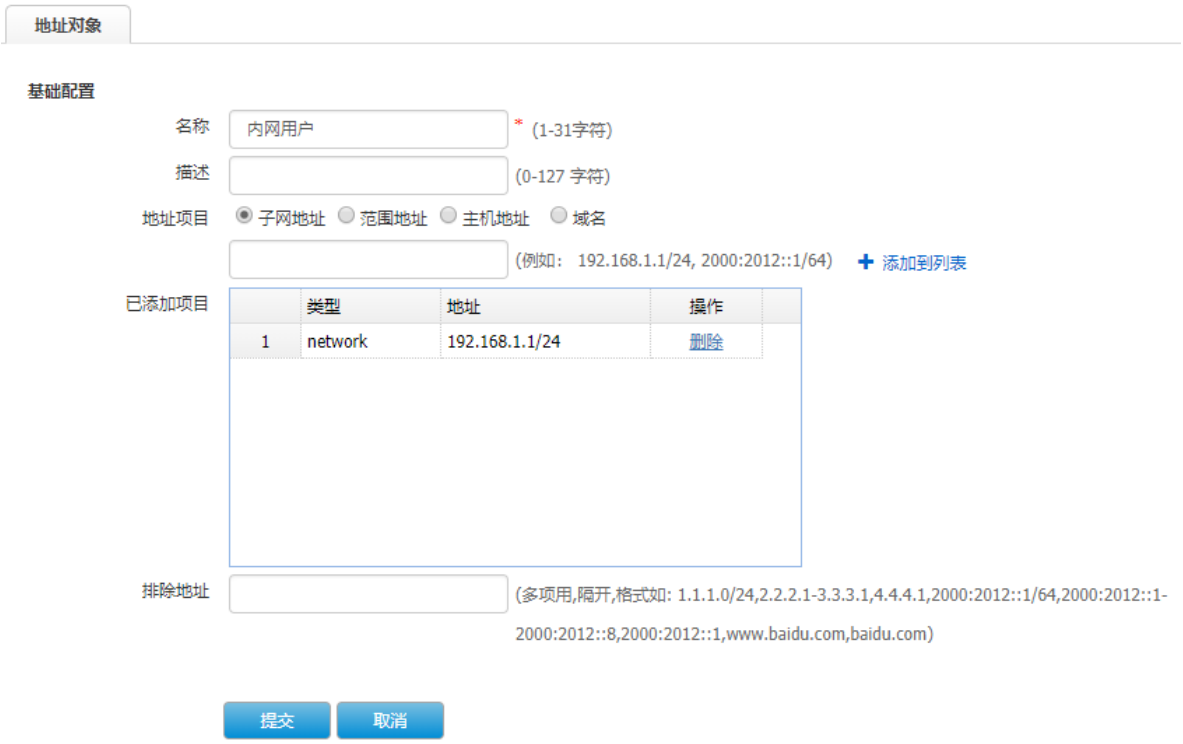
如图 1-92 所示，进入“网络配置 > 路由管理 > 静态路由”页面，新建一条访问外网的默认路由。

图1-92 配置静态路由

(3) 配置地址对象

如图 1-93 所示，进入“策略配置 > 对象管理>地址对象>地址对象”页面，点击<新建>按钮创建内网用户地址对象，设置地址为 192.168.1.0/24，点击<提交>。

图1-93 配置地址对象



(4) 配置用户识别范围

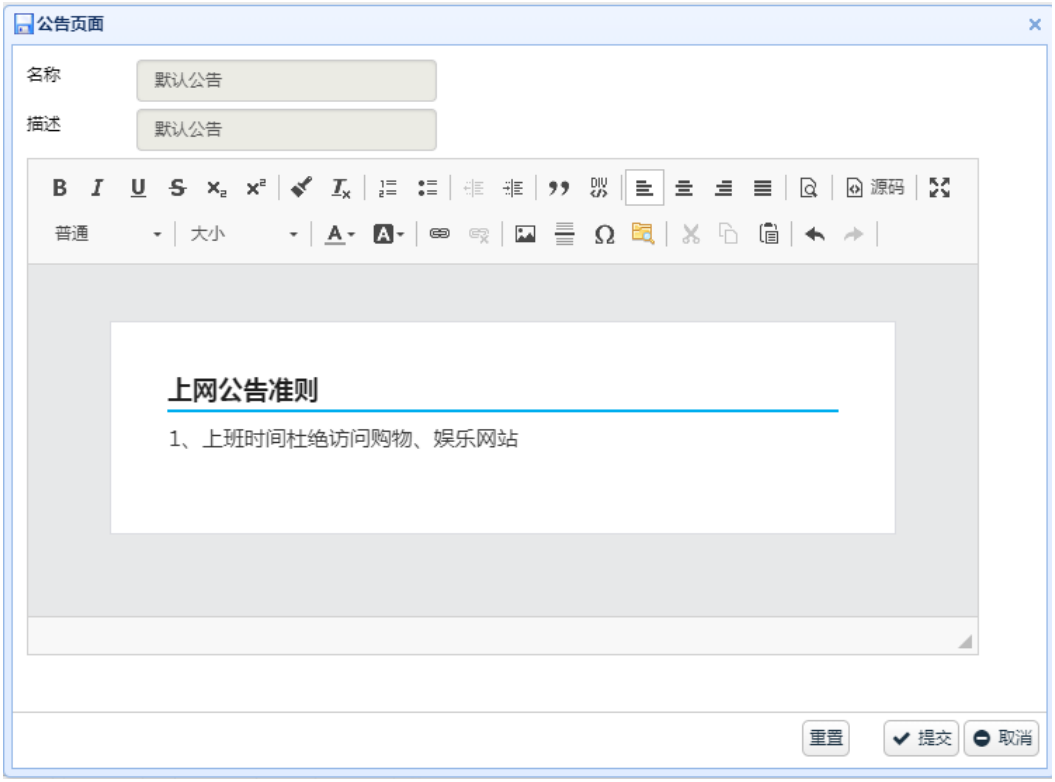
如图 1-94 所示，进入“用户管理 > 认证管理 > 高级选项 > 全局配置”页面，识别范围选择“内网用户”，其它配置默认，提交配置。

图1-94 用户识别范围

(5) 配置自定义公告内容

如图 1-95 所示，进入“策略配置 > 对象管理 > 公告页面”，点击名称中“默认公告”，弹出自定义公告编辑页面。

图1-95 自定义公告



(6) 开启终端公告推送功能

如图 1-96 所示，进入“策略配置 > 控制策略”页面，新建控制策略，源 IP 选择“内网用户”并开启终端公告推送功能。

图1-96 移动终端推送配置

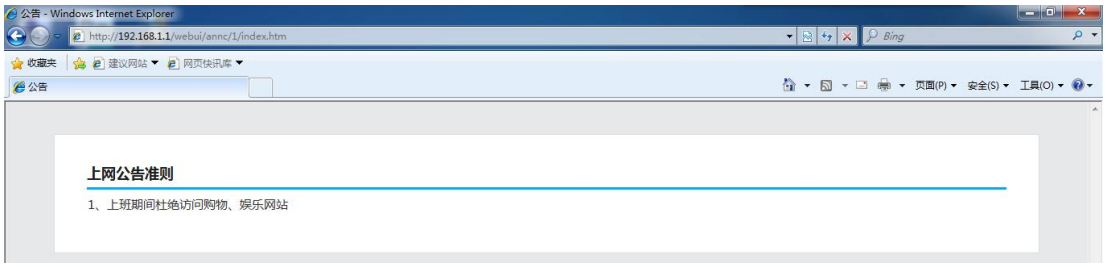
4. 配置注意事项

- 内网接口管理方式必须开启 http，终端才能正常访问公告页面。

5. 验证配置

如图 1-97 所示，某员工使用 1 台 PC 访问 http 网站，会被推送上网准则公告。

图1-97 推送公告



1.9 高级配置

1.9.1 高级配置简介

高级配置包含时间、老化时间、终端配置，时间中引用时间对象以控制策略的生效时间，老化时间控制命中此控制策略的会话存活周期，终端可以控制当前控制策略基于哪些类型的终端生效。

1.9.2 高级配置页面

通过菜单“策略配置>控制策略”，新建一条控制策略，点击<高级配置>，进入如图 1-98 所示页面。各个配置项含义如表 1-23 所示。

图1-98 高级配置页面

表1-23 高级配置各项含义表

标题项	说明
时间	策略生效时间，可以引用时间对象。
老化时间	基于策略的老化时间，命中此策略的会话按此时间进行老化，默认为0。
终端	终端型号，包含any、移动终端、PC、多终端。
终端型号	选择终端型号，默认为any。此功能依赖于第三方用户同步中的ddi终端用户功能，需要将终端型号信息同步给设备。

点击<选择终端>，弹出如图 1-99 所示页面。各个配置项含义如表 1-24 所示。

图1-99 选择终端页面

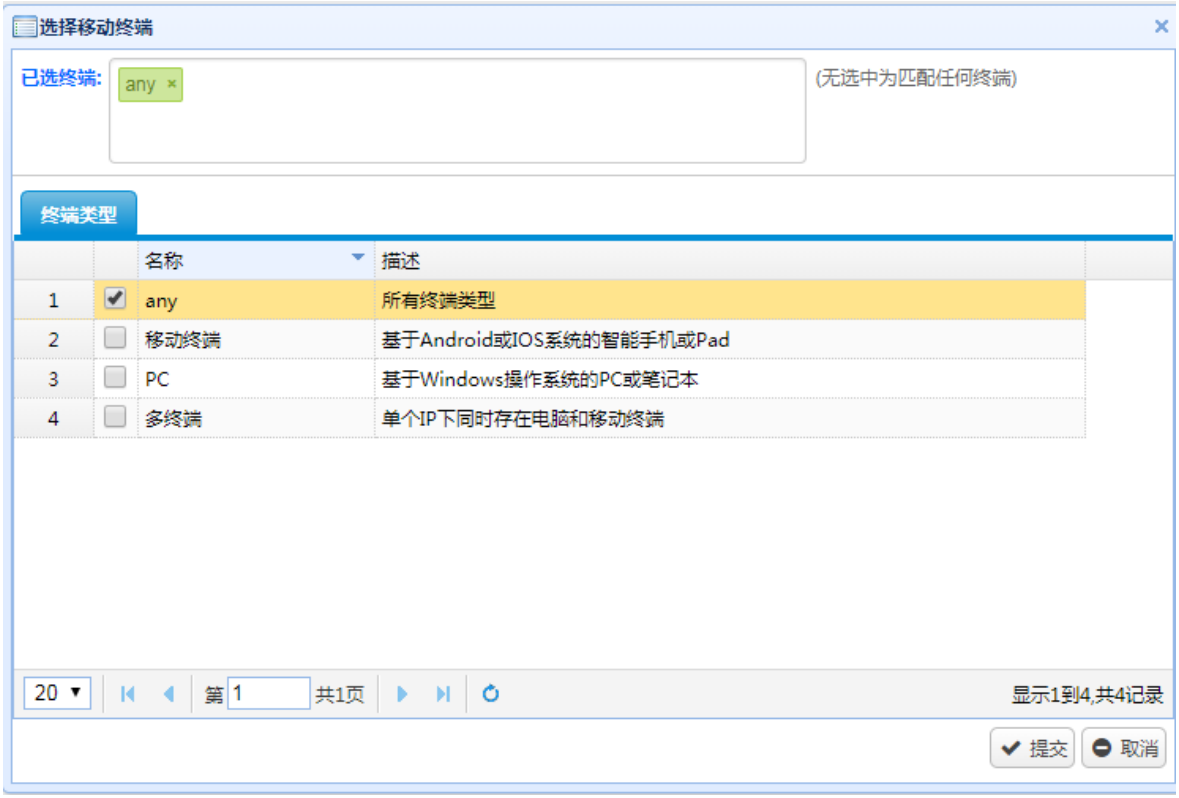


表1-24 选择终端各项含义表

标题项	说明
已选终端	显示已选择的终端类型配置。
终端类型	终端类型包含： • any：所有终端类型。 • 移动终端：基于 Android 或 IOS 系统的智能手机或 Pad。 • PC：基于 Windows 操作系统的 PC 或笔记本。 • 多终端：单个 IP 下同时存在 PC 和移动终端。
名称	终端类型的名称。
描述	终端类型实际含义的描述信息。

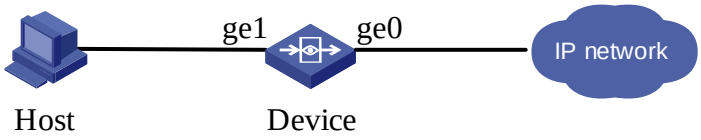
1.9.3 终端控制配置举例

1. 组网需求

针对公司内部网络，不允许移动终端用户通过 WIFI 热点接入（如 360wifi），进行上网，防止降低工作效率。

2. 组网图

图1-100 终端控制组网图



3. 配置步骤

(1) 创建终端控制策略，在导航栏中选择“策略配置 > 控制策略”，点击<新建>进入控制策略配置页面，行为选择“拒绝”，高级配置中的终端选择“移动终端”，如图 1-101 所示。

图1-101 终端控制策略

(2) 点击<提交>按钮，提交配置。

4. 验证配置

在办公电脑上，启用 360wifi，使用移动终端连接 wifi，访问网页，被阻断，PC 端可以正常访问网络，如图 1-102、图 1-103 所示。

图1-102 移动终端上网被阻断

图1-103 PC 端可以正常访问网络

目 录

1 控制策略分析 1
1.1 控制策略分析概述 1
1.2 控制策略全局分析 1
1.3 控制策略即时分析 5
1.4 策略分析配置举例 8

1 控制策略分析

1.1 控制策略分析概述

控制策略分析对当前存在或即将新建的策略进行分析，查看现有环境中有：冲突、冗余、隐藏、合并、过期和空策略中的哪一种情况，让设备更易于使用、便于维护和管理。

策略分析针对策略内的用户、源接口、目的接口、源地址、应用、服务、目的地址和时间进行对象内逐一分析。策略分析的结果包括六类：

- 冲突策略：不区分匹配的前后顺序，若策略 A 和策略 B 存在数据流交集（非包含和被包含关系），且 AB 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 策略包含在里面，删除 A 策略不会对其余策略产生影响，如果 AB 策略行为相同，那么 A 策略会被计算为冗余策略；
- 隐藏策略：根据匹配的前后顺序（先匹配 A 策略在匹配 B 策略），如果 B 策略匹配的所有数据流会被 A 策略包含在里面，如果 AB 策略行为相同，那么 B 策略会被计算为隐藏策略；
- 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）的情况下，则认为是可以合并的策略；
- 空策略：当策略中匹配的任何一个对象为空时，那么该策略会被计算为空策略；
- 过期策略：发现当前策略中，匹配的时间范围已经不会再次出现的策略。

策略分析分为全局分析和单独策略的即时分析两种方式。

1.2 控制策略全局分析

在导航栏中选择“策略配置>控制策略>策略分析”，进入控制策略分析显示界面，如图 1-1 所示。

图1-1 控制策略分析显示界面

控制策略分析的含义如表 1-1 所示：

表1-1 控制策略分析显示信息描述表

标题项	说明
策略分析设置	点击 ⚙ 按钮，可以根据周期进行配置自动分析。
立即分析	立即进行控制策略分析。
策略问题数量	用柱状图进行分类显示存在问题的策略数量。
策略宽松度分析	用柱状图进行分类显示策略中源地址和目的地址的宽松度。
冲突策略	显示当前策略中存在的冲突策略信息。
冗余策略	显示当前策略中存在的冗余策略信息。
隐藏策略	显示当前策略中存在的隐藏策略信息。
可合并策略	显示当前策略中存在的可合并策略信息。
空策略	显示当前策略中存在的空策略信息。

标题项	说明
过期策略	显示当前策略中存在的过期策略信息。
忽略策略	显示当前策略中存在的忽略策略信息。
状态	控制策略的状态： • 表示策略启用 • 表示策略禁用
ID	控制策略的ID。
行为	控制策略行为的状态包含： • 允许 • 拒绝
策略组	匹配控制策略匹配的时间对象。
用户	匹配控制策略的用户对象。
源接口/域	匹配控制策略的源接口/域。
目的接口/域	匹配控制策略的目的接口/域。
源地址	匹配控制策略的源地址。
目的地址	匹配控制策略的目的地址。
应用	匹配控制策略的应用对象。
服务	匹配控制策略的服务对象。
终端	匹配控制策略匹配的终端类型，包括：any、移动终端、PC、多终端。 移动终端：基于Android或IOS系统的智能手机或Pad； PC：基于Windows操作系统的PC或笔记本； 多终端：单个IP下同时存在电脑和移动终端。
描述	控制策略描述。
匹配次数	匹配控制策略的次数。
应用安全	如果显示图标，表示已经配置应用过滤或URL过滤规则。
时间	匹配控制策略匹配的时间对象。
日志	控制策略行为选择为拒绝时是否记录日志。
老化时间	基于控制策略的老化时间，缺省情况下，老化时间为0，表示使用各个协议默认的老化时间。
操作	控制策略支持的操作，包含编辑和忽略策略设置。

策略分支支持定时分析，在导航栏中选择“策略配置>控制策略>策略分析”，进入控制策略分析页面，点击策略分析设置，如图 1-2 所示。

图1-2 策略分析设置界面

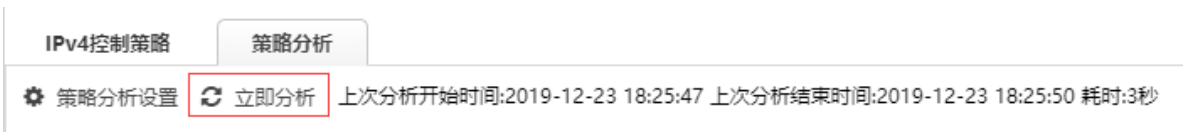
策略分析设置界面的详细信息如表 1-2 所示：

表1-2 策略外部编辑界面详细信息

标题项	说明
开启分析	开启/关闭策略定时分析。
CPU高于	配置范围（50-99）内，当CPU高于配置信息后自动策略分析停止。
内存高于	配置范围（50-99）内，当内存高于配置信息后自动策略分析停止。
周期	可以选择每天、每周、每月。
时间	可以选择定时自动分析的时间。

策略分析界面默认显示上次的分析结果，单击<立即分析>按钮，可以对整体的策略进行策略分析，如图 1-3 所示。

图1-3 策略立即分析配置界面



控制策略分析完成后会显示开始分析时间和分析结束时间，并显示耗时时长，如表 1-3 所示。

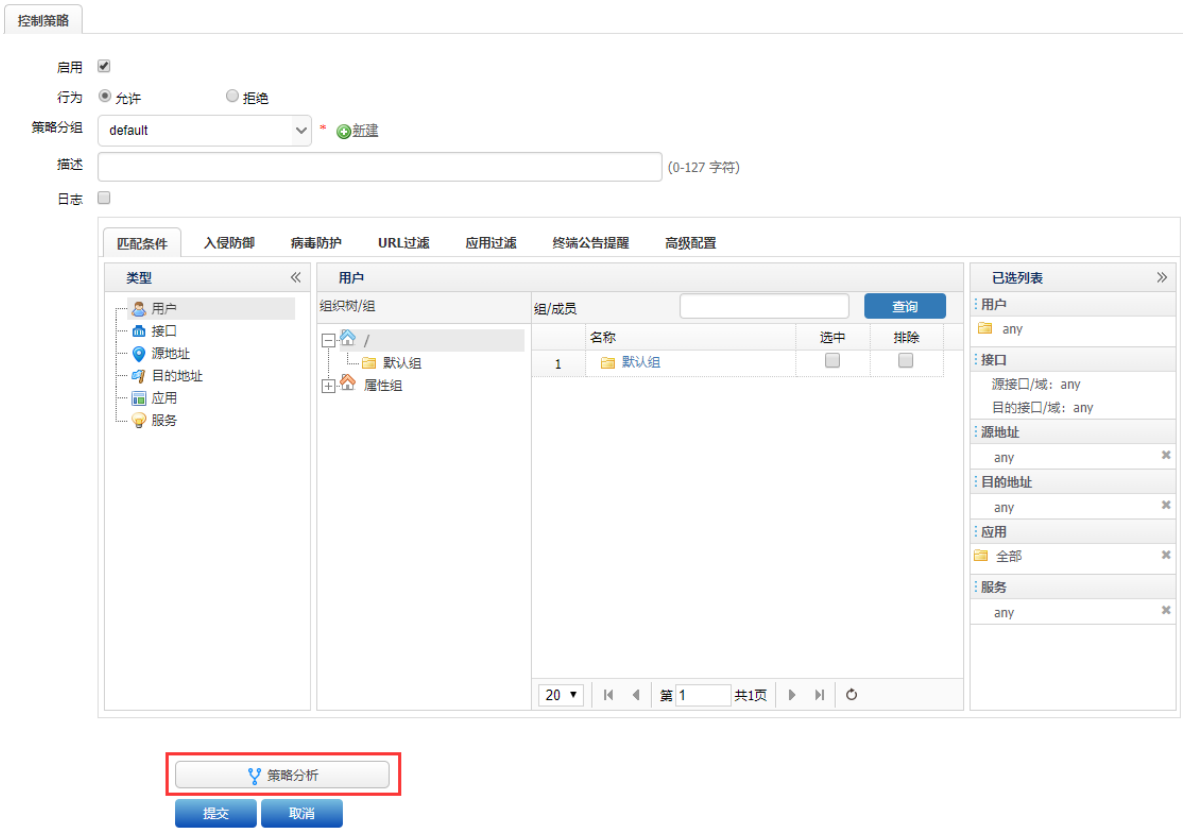
表1-3 控制策略立即分析完成后显示信息

标题项	说明
上次分析开始时间	显示上次开始分析的时间。
上次分析结束时间	显示上次分析结束的时间。
耗时	显示总耗时为多长时间。

1.3 控制策略即时分析

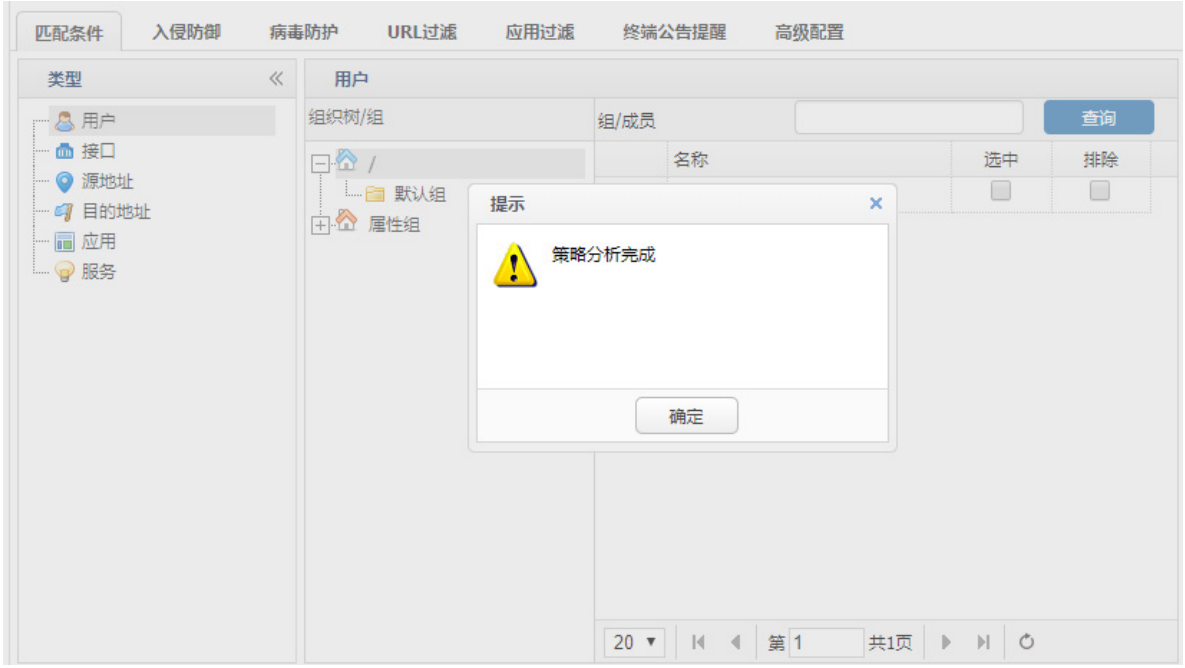
在导航栏中选择“策略配置>控制策略”，点击新建按钮，进入控制策略配置显示界面，如图 1-4 所示。

图1-4 控制策略配置界面



控制策略配置完成后，点击<策略分析>按钮，进行即时分析并显示分析进度条，分析完成后弹出策略分析完成的提示，如图 1-5 所示。

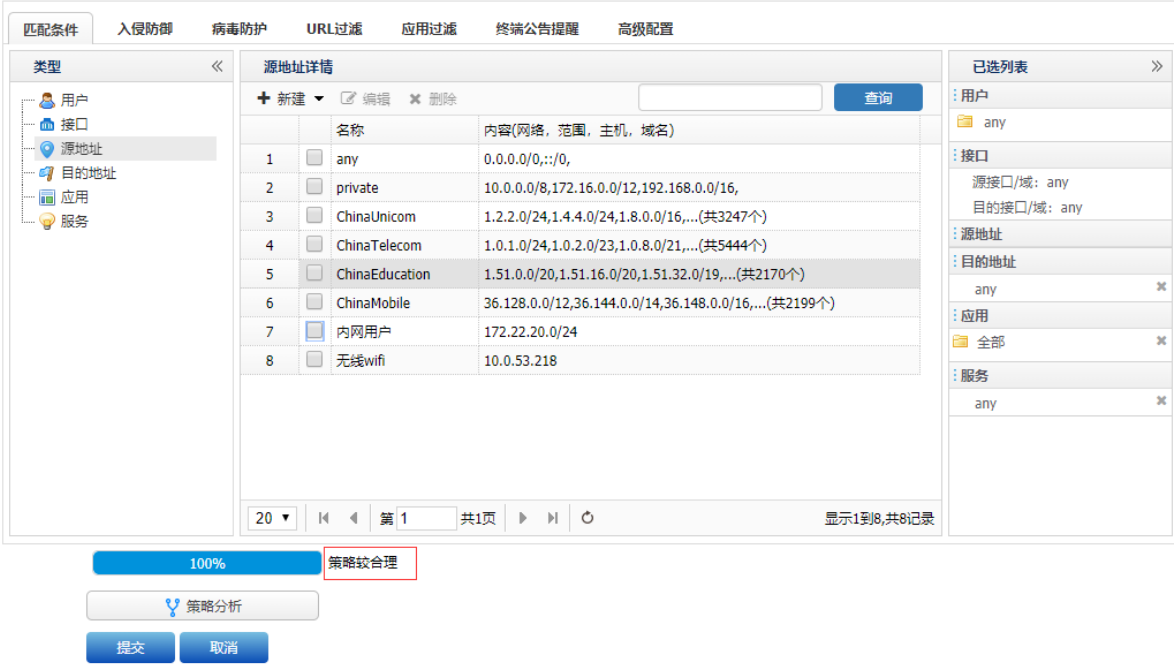
图1-5 控制策略即时分析界面



如当前策略和已存在策略存在影响，会在页面显示分析结果。点击分析结果，会显示当前策略和哪些策略存在影响关系，如图 1-6 所示。如果当前策略和已存在策略互不影响，则会显示策略较合理，如图 1-7 所示。

图1-6 控制策略即时分析结果

图1-7 控制策略即时分析结果-策略合理



策略分析结果中异常策略详细信息如表 1-4 所示：

表1-4 异常策略详细信息描述

标题项	说明
冲突策略	不区分匹配的前后顺序，若策略A和策略B存在数据流交集（非包含和被包含关系），且AB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策略包含在里面，删除A策略不会对其余策略产生影响，如果AB策略行为相同，那么A策略会被计算为冗余策略。
隐藏策略	根据匹配的前后顺序（先匹配A策略在匹配B策略），如果B策略匹配的所有数据流会被A策略包含在里面，如果AB策略行为相同，那么B策略会被计算为隐藏策略。
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）的情况下，则认为是可以合并的策略。
空策略	当策略中匹配的任何一个对象为空时，那么该策略会被计算为空策略。
过期策略	发现当前策略中，匹配的时间范围已经不会再次出现的策略。
忽略策略	手动忽略不进行分析的策略。

1.4 策略分析配置举例

1. 用户需求

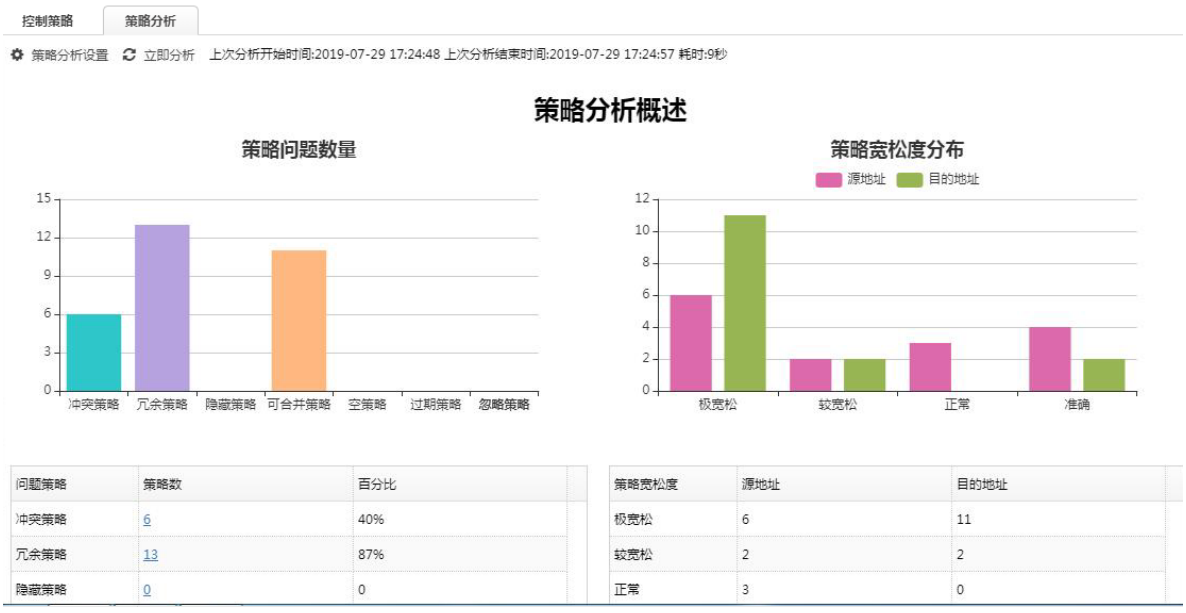
某公司当前策略比较多，对当前所有策略进行分析查看有哪些异常策略，可以对控制策略进行梳理如图 1-8 所示。

图1-8 某公司内网控制策略

2. 结果验证

进入策略分析页面，点击立即分析按钮，当分析完成后可以看到该公司策略存在哪些异常策略方便管理员进行维护和修改，如图 1-9 所示

图1-9 某公司策略分析结果展示



问题策略	策略数	百分比
冲突策略	6	40%
冗余策略	13	87%
隐藏策略	0	0

策略宽松度	源地址	目的地址
极宽松	6	11
较宽松	2	2
正常	3	0

目 录

1 IPv6 网络……1-1
1.1 IPv6 路由通告……1-1
1.2 IPv6 隧道……1-3
1.3 IPv6 静态路由……1-5
1.4 IPv6 路由表……1-6
1.5 IPv6 异常包攻击防御……1-7
1.6 典型配置举例……1-8
1.6.1 路由通告配置举例……1-8
1.6.2 IPv6 隧道配置举例……1-10
1.6.3 IPv6 静态路由典型配置举例……1-11

1 IPv6 网络

1.1 IPv6 路由通告

通过菜单“网络配置 > 基础网络 > IPv6 网络 > IPv6 路由通告”，进入路由通告信息显示页面。如图 1-1 所示。

图1-1 IPv6 路由通告信息显示

	接口名称	IPv6地址	发布路由通告	发布间隔	被管理标记	其他标记	路由前	操作
2	ge0		不发布	198-600	无标记	无标记		
3	ge1		不发布	198-600	无标记	无标记		
4	ge2		不发布	198-600	无标记	无标记		
5	ge3		不发布	198-600	无标记	无标记		
6	ge4		不发布	198-600	无标记	无标记		
7	ge5		不发布	198-600	无标记	无标记		
8	ge6		不发布	198-600	无标记	无标记		
9	ge7		不发布	198-600	无标记	无标记		
10	ge8		不发布	198-600	无标记	无标记		

点击<编辑>按钮，进入如图 1-2 所示的路由通告信息配置页面。各个配置项的含义如表 1-1 所示。

图1-2 路由通告配置页面

表1-1 路由通告信息配置项含义描述表

标题项	说明
接口名称	配置发布路由通告的接口名称。
发布路由通告	是否发布路由通告，如果选中，则发布，否则不发布。
发布间隔	配置发布路由通告的最大间隔，最小间隔是最大时间间隔的三分之一。
默认路由器时间	PC把发布通告的路由器作为默认路由的下一跳的时间。
邻居可达时间	通告的邻居可达时间，如果为0，则表示路由器不指定邻居可达时间。
NS重传间隔	通告的NS重传间隔，如果为0，则表示路由器不指定NS重传间隔。
MTU	通告的链路MTU值，如果为0，则表示不通告链路MTU。
跳数	通告的hop-limit值。
被管理标记	如果选中被管理标记，则表示PC不使用通告的前缀进行无状态地址自动配置。
其它标记	如果选中其它配置标记，则表示PC应该向DHCPv6服务器请求DNS配置信息。

如需添加新的路由前缀，可点击“前缀信息配置”框中的<新建>按钮，进入如图 1-3 所示的配置页面。通过该页面添加前缀信息，各个配置项的含义如表 1-2 所示。

图1-3 前缀信息配置页面

表1-2 前缀信息各个配置项含义描述表

标题项	说明
路由前缀	通告的网段前缀，PC可使用该前缀进行无状态地址自动配置。
有效生存期	通过该网段前缀进行无状态地址自动配置生成地址后，该地址的有效时间。
首选生存期	通过该网段前缀进行无状态地址自动配置生成地址后，该地址的优先使用时间。
在链路标记	如果选中该标记，则表示可使用该前缀进行判定是否与其它主机在同一链路上。
自治标记	如果选中该标记，则表示可使用该前缀进行无状态地址自动配置。

1.2 IPv6隧道

通过菜单“网络配置 > 基础网络 > IPv6 网络 > IPv6 隧道”，进入 IPv6 隧道页面，如图 1-4 所示。在该页面上可以新建、编辑、删除、浏览 IPv6 隧道。

图1-4 IPv6 隧道概览页面

点击<新建>按钮，进入 IPv6 隧道的新建页面，如图 1-5 所示。各个配置项的含义如表 1-3 所示。

图1-5 IPv6 隧道新建页面

表1-3 IPv6 隧道各个配置项含义描述表

标题项	说明
名称	tunnel前缀加上tunnel id即为tunnel接口的名称。
隧道模式	该隧道采用的隧道模式，有三种模式，分别为： • 手动隧道； • isatap 隧道； • 6to4 隧道。
隧道源	指定封装隧道报文时，用哪个地址作为外层的源IPv4地址。 可以使用指定的地址作为隧道源地址，也可以使用某个接口的主IP地址作为隧道源地址。
源地址	指定封装隧道报文时，作为外层封装的IPv4报文的源地址。
隧道目的	指定封装隧道报文时，作为外层封装的IPv4报文的目的地址。
IPv6地址	配置隧道接口的IPv6主地址，只有隧道模式选择istap模式才需要配置。

点击<提交>按钮，提交配置。提交配置后可在如图 1-6 所示的页面上查看配置的 IPv6 隧道信息。

图1-6 IPv6 隧道信息

点击<编辑>按钮，可对选中条目进行编辑。

点击<删除>按钮，可对选中条目进行删除。

1.3 IPv6静态路由

通过菜单“网络配置 > 基础网络 > IPv6 网络 > IPv6 静态路由”，进入 IPv6 静态路由页面，如图 1-7 所示。在该页面上可以新建、删除、浏览 IPv6 静态路由。

图1-7 IPv6 静态路由页面

点击<新建>按钮，进入 IPv6 静态路由的新建页面，如图 1-8 所示。各个配置项的含义如表 1-4 所示。

图1-8 IPv6 静态路由新建页面

表1-4 IPv6 静态路由各项配置含义描述表

标题项	说明
目的前缀	静态路由的目的网络前缀。
掩码长度	静态路由的目的网络的前缀长度。
下一跳/出接口	静态路由的下一跳，为IP地址或接口。
下一跳	静态路由的下一跳使用指定的地址作为网关地址。
出接口	静态路由的下一跳使用指定的接口作为下一跳的出接口。

点击<提交>按钮，提交配置。提交配置后可在如图 1-9 所示的页面上查看配置的 IPv6 静态路由信息。

图1-9 IPv6 静态路由信息

点击<删除>按钮，可对选中条目进行删除。

说明

: 该图标表示该条静态路由有效。

: 该图标表示该条静态路由无效。

1.4 IPv6路由表

通过菜单“网络配置 > 基础网络 > IPv6 网络 > IPv6 路由表”，进入 IPv6 路由表，如图 1-10 所示。在该页面上可以浏览所有 IPv6 路由。

图1-10 IPv6 路由表

说明

：该图标表示该条静态路由有效。

：该图标表示该条静态路由无效。

1.5 IPv6异常包攻击防御

通过菜单“策略配置 > 安全设置 > 安全防护 > 异常包攻击防御 > IPv6 异常包攻击防御”，进入 IPv6 异常包攻击防御，如图 1-11 所示。在该页面上可以配置 IPv6 异常包攻击防御。各个配置项的含义如表 1-5 所示。

图1-11 IPv6 异常包攻击防御配置页面

表1-5 IPv6 异常包攻击防御配置项含义描述表

标题项	说明
Winnuke	winnuke报文攻击。
Land-Base	Land-base报文攻击。
TCP flag	异常的TCP flag报文攻击。
Fraggle	fraggle报文攻击。
IP spoof	IP地址欺骗攻击。

1.6 典型配置举例

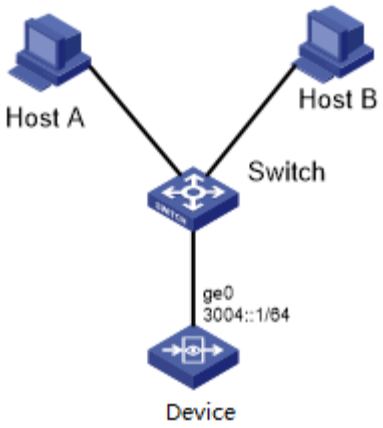
1.6.1 路由通告配置举例

1. 组网需求

要求设备发布路由通告信息，对网络内的主机进行无状态地址自动配置。

2. 组网图

图1-12 路由通告配置组网图



3. 配置思路

- 在设备的接口 ge0 上配置 RA，发布前缀为 3004::/64 的前缀。
- HostA 和 HostB 收到设备的 RA 信息，自动生成前缀为 3004::1/64 的 IPv6 地址。

4. 配置步骤

按图 1-13 所示配置路由通告。

图1-13 配置路由通告

5. 配置验证

在设备上使用 **display ipv6 rtadv-conf** 验证配置结果。

```
host# display ipv6 rtadv-conf ge0
ipv6 nd rtadv disable (suppress ra)
 ---------------------------------------------------
 Field-name                Value              Units
 ---------------------------------------------------
 link-mtu                  0             byte
 hop-limit                 64            -
 ra-maxinterval            600           second
 ra-mininterval            198           second
 reachable-time            0             millisecond
 ns-retrans-interval       0             millisecond
 other-config-flag         false         -
 managed-config-flag       false         -
 default-rt-lifetime       1800          second

--------------------------------------------------------------------------------
```

```
Prefix                  Valid-lifetime       Preferred-lifetime     On-link     Autonomous
--------------------------------------------------------------------------------------------
3004::/64               2592000              604800                 true        true
```

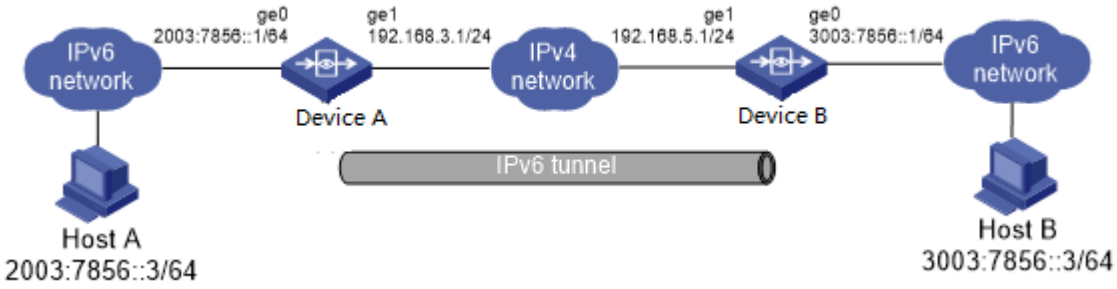
1.6.2 IPv6 隧道配置举例

1. 组网需求

如图 1-14 所示，两个 IPv6 网络分别通过设备 A 和设备 B 与 IPv4 网络连接，设备 A 与设备 B 之间路由可达，要求在设备 A 和设备 B 之间建立 IPv6 手动隧道，使两个 IPv6 网络可以互通。

2. 组网图

图1-14 IPv6 手动隧道组网图



3. 配置步骤

(1) 按照图 1-14 组网。

(2) 设备 A 配置 IPv6 手动隧道。如图 1-15 所示。

图1-15 设备 A 配置页面

(3) 配置设备 B 手动隧道。如图 1-16 所示。

图1-16 配置设备 B 手动隧道

(4) 配置主机。

配置 Host A 的 IPv6 地址为 2003:7856::3/64，默认网关配置为设备 A 的 ge0 口的地址 2003:7856::1。

配置 Host B 的 IPv6 地址为 3003:7856::3/64，默认网关配置为设备 B 的 ge0 口的地址 3003:7856::1。

4. 验证配置

在 HostB 上 ping 2003:7856::3 来验证。

```
hostA# ping6 2003:7856::3
PING 2003:7856::3 (3003:7856::3) 56 data bytes
      seq       ttl     time(ms)
        1       128     1.178
        2       128     1.339
        3       128     1.053
        4       128     1.111
        5       128     1.170

--- 2003:7856::3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.053/1.170/1.339/0.098 ms
```

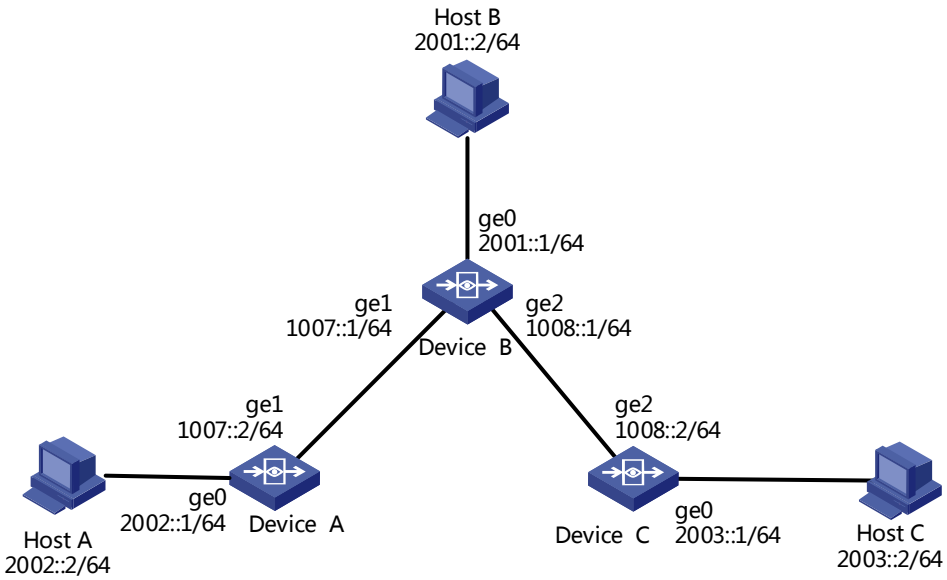
1.6.3 IPv6 静态路由典型配置举例

1. 组网需求

要求各问题重复之间配置 IPv6 静态路由协议后，可以使所有主机和问题重复之间互通。

2. 组网图

图1-17 静态路由典型组网图



3. 配置步骤

(1) 如图 1-17 所示，给各个设备的相应接口上配置 IPv6 地址（略）。

(2) 配置 IPv6 静态路由。

在设备 A 上配置 IPv6 缺省路由，如图 1-18 所示。

图1-18 配置设备 A 静态路由

在设备 B 上配置静态路由。如图 1-19 所示。

图1-19 配置设备 B 静态路由

在设备 C 上配置静态路由。如图 1-20 所示。

图1-20 配置设备 C 静态路由

(3) 配置主机地址和网关。

根据组网图配置好各主机的 IPv6 地址，并将 HostA 的缺省网关配置为 2002::1，HostB 的缺省网关配置为 2001::1/64，HostC 的缺省网关配置为 2003::1。

4. 验证配置

在设备 B 上执行 ping6 命令验证。

```
hostB# ping6 2002::2
PING 2002::2 (2002::2) 56 data bytes
      seq       ttl     time(ms)
        1       128     1.178
        2       128     1.339
        3       128     1.053
        4       128     1.111
        5       128     1.170

--- 2002::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.053/1.170/1.339/0.098 ms
```

目 录

1 NAT 1-1
1.1 NAT 概述 1-1
1.1.1 地址转换控制 1-1
1.1.2 NAT 实现 1-1
1.1.3 NAT64/46 1-1
1.2 NAT 地址池配置 1-2
1.3 源 NAT 配置 1-3
1.4 目的 NAT 配置 1-4
1.5 静态 NAT 配置 1-5
1.6 NAT64 1-6
1.7 NAT46 1-7
1.8 配置举例 1-8
1.8.1 源 NAT 配置案例 1-8
1.8.2 目的 NAT 配置案例 1-11
1.8.3 静态 NAT 配置案例 1-16

1 NAT

1.1 NAT概述

NAT 的配置分为：源地址转换（Source）、目的地址转换（Destination）及静态地址转换（Static）三种类型。

每条 NAT 规则都是和某个特定的接口关联的，需要注意的是，源地址转换是在离开接口时进行转换的，目的地址转换是在进入接口时进行转换的，所以配置源地址转换的时候必须和对应的出接口关联，而配置目的地址转换的时候需要和对应的入接口关联。

源 NAT、目的 NAT、静态 NAT 均支持 IPv4 和 IPv6 网络。

1.1.1 地址转换控制

在实际应用中，我们可能希望某些内部网络的主机可以访问外部网络，而某些主机不允许访问，即当 NAT 设备查看 IP 数据报文的报头内容时，如果发现源 IP 地址属于禁止访问外部网络的内部主机，它将不进行地址转换。另外，也希望只有指定的公网地址才可用于地址转换。

设备可以 NAT 规则的匹配条件和 NAT 地址池来对地址转换进行控制。

- 匹配条件可以有效地控制地址转换的使用范围，只有满足匹配条件的数据报文才可以进行地址转换。
- 地址池是用于地址转换的一些连续的公网 IP 地址的集合，它可以有效地控制公网地址的使用。用户可根据自己拥有的合法 IP 地址数目、内部网络主机数目以及实际应用情况，定义合适的地址池。在地址转换的过程中，NAT 设备将会从地址池中挑选一个 IP 地址作为数据报文转换后的源 IP 地址。

1.1.2 NAT 实现

通过创建并执行 NAT 规则来实现 NAT 功能。NAT 规则有三类，分别为源 NAT 规则、目的 NAT 规则和静态 NAT 规则。源 NAT 转换源 IP 地址，从而隐藏内部 IP 地址或者分享有限的 IP 地址；目的 NAT 转换目的 IP 地址，通常是将受保护的内部服务器的 IP 地址转换成公网 IP 地址；静态转换是指将内部网络的私有 IP 地址转换为公有 IP 地址，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只转换为某个公有 IP 地址。

1.1.3 NAT64/46

NAT64 是通过在两个地址族之间执行 IP 头和地址转换，促进 IPv6-only 和 IPv4-only 主机和网络之间的通信。内容提供商通过部署 NAT64/46 技术可透明地向 IPv6 互联网用户提供现有的或者新的服务，现有网络基础设施几乎不需要做太大的改动，从而保持业务连续性。

通过 NAT 转换，实现从 IPv6 到 IPv4 网络的互联互通。使用场景如下：

- NAT64 转换

NAT64 转换，完成 IPv6 网络主机对 IPv4 网络主机访问的地址转换。

网络访问由 IPv6 主机或网络发起。

- NAT46 转换

NAT46 转换，完成 IPv4 网络主机对 IPv6 网络主机访问的地址转换。

网络访问由 IPv4 主机或网络发起。

1.2 NAT地址池配置

在导航栏中选择“策略配置 > NAT 转换策略 > 地址池”，进入地址池的显示页面，如图 1-1 所示。

单击<新建>按钮，进入地址池的配置页面，如图 1-2 所示。地址池详细配置说明，如表 1-1 所示。

图1-1 地址池显示界面

图1-2 新建地址池界面

表1-1 地址池详细配置

标题项	说明
地址类型	选择地址类型为IPv4或者IPv6
名称	NAT地址池的名称
地址项目	NAT地址池中的起始地址和结束地址，NAT地址池中的结束地址不能小于起始地址。从起始地址到结束地址这个范围内的地址都会作为地址池中的地址
地址池	显示已加入地址池的地址

1.3 源NAT配置

在导航栏中选择“策略配置 > NAT 转换策略 > 源 NAT”，单击<新建>按钮，进入源 NAT 配置页面，如图 1-3 所示。源 NAT 详细配置说明，如表 1-2 所示。

图1-3 源 NAT 配置

表1-2 源 NAT 详细配置

标题项	说明
启用	勾选后启用NAT策略，默认是勾选状态。
地址类型	选择地址类型为IPv4或者IPv6。
源地址	NAT规则匹配的源地址，可以是地址节点或地址组。

标题项	说明
启用	勾选后启用NAT策略，默认是勾选状态。
服务	NAT规则匹配的服务名，可以是服务资源或服务组。
接口	NAT规则匹配的出接口名。
转换类型	需要转换成的地址，可以选择转换成出接口地址、地址池中的地址或不转换 不转换：为NAT白名单，指定的地址不做地址转换。
日志	是否需要对该规则启用日志。

1.4 目的NAT配置

在导航栏中选择“策略配置 > NAT 转换策略 > 目的 NAT”，单击<新建>按钮，进入目的 NAT 配置页面，如图 1-4 所示。目的 NAT 详细配置说明，如表 1-3 所示。

图1-4 目的 NAT 配置

表1-3 目的 NAT 详细配置

标题项	说明
启用	勾选后启用NAT策略，默认是勾选状态
地址类型	选择地址类型为IPv4或者IPv6
源地址	NAT规则匹配的源地址，可以是地址节点或地址组
目的地址	NAT规则匹配的目的地址，可以是地址节点或地址组
服务	NAT规则匹配的服务名，可以是服务资源或服务组
接口	NAT规则匹配的出接口名
转换类型	需要转换成的地址，可以选择地址映射、端口映射或不转换 不转换：为NAT白名单，指定的地址不做地址转换
日志	是否需要对该规则启用日志
发布服务器	NAT回流功能，允许内网用户以外网IP来访问内网服务器，开启后此目的NAT匹配不关心报文入接口，同时会在报文出接口做源NAT转换，转换地址为出接口地址。

1.5 静态NAT配置

在导航栏中选择“策略配置 > NAT 转换策略 > 静态 NAT”，单击<新建>按钮，进入静态 NAT 配置页面，如图 1-5 所示。静态 NAT 详细配置说明，如表 1-4 所示。

图1-5 静态 NAT 配置

表1-4 静态 NAT 详细配置

标题项	说明
启用	勾选后启用NAT策略，默认是勾选状态
地址类型	选择地址类型为IPv4或者IPv6
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
外部接口	和外部网络相连的接口名
日志	是否需要对该规则启用日志

1.6 NAT64

在导航栏中选择“策略配置 > NAT 转换策略> NAT64”，单击<新建>按钮，进入 NAT64 配置页面，如下图所示。。

图1-6 NAT64 配置

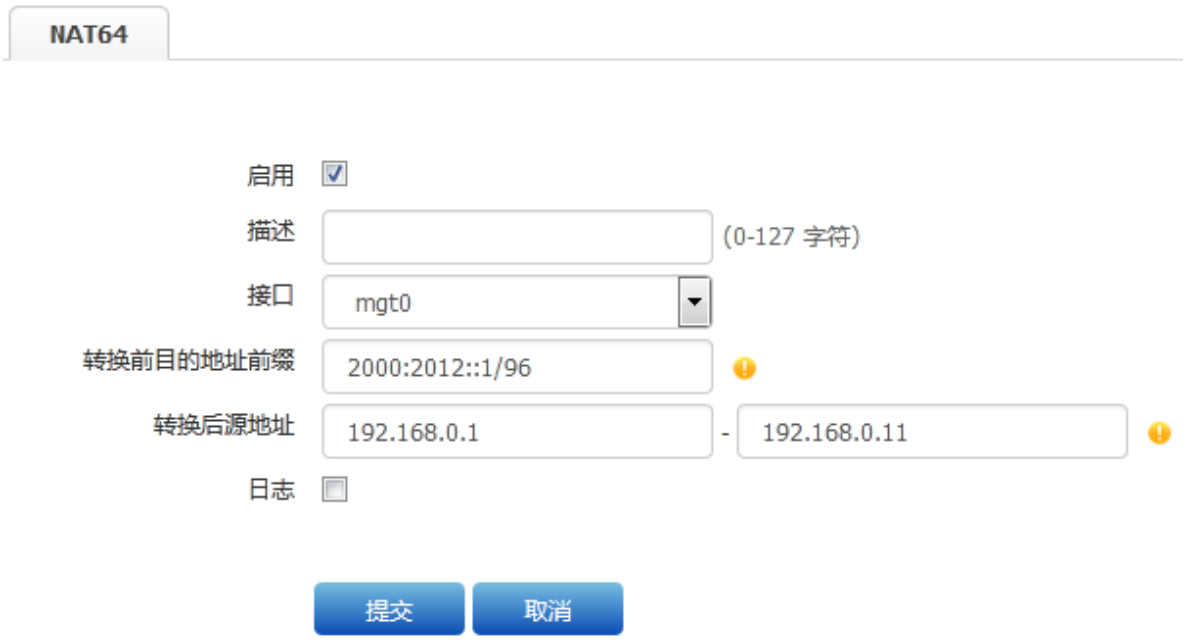


表1-5 NAT64 详细配置

标题项	说明
启用	是否启用NAT64策略。
接口	策略匹配的接口

标题项	说明
转换前目的地址前缀	策略匹配的目的地址IPv6前缀
转换后源地址	策略匹配后源地址转换IPv4地址池
日志	是否发生日志

1.7 NAT46

在导航栏中选择“策略配置 > NAT 转换策略> NAT46”，单击<新建>按钮，进入 NAT46 配置页面，如下图所示。

图1-7 NAT46 配置

表1-6 NAT46 详细配置

项目	说明
启用	是否启用NAT46策略。
接口	策略匹配的接口
转换前目的地址	策略匹配的IPv4目的地址
转换后源地址前缀	策略匹配后源地址转换IPv6地址前缀
转换后目的地址	策略匹配后转换的IPv6目的地址

日志	是否发生日志

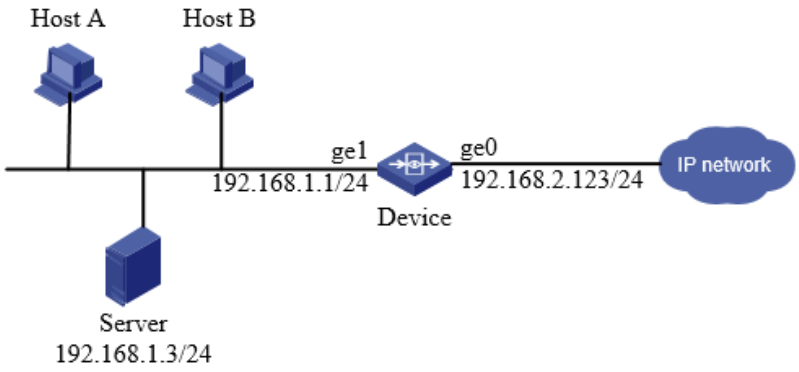
1.8 配置举例

1.8.1 源 NAT 配置案例

1. 组网需求

公司拥有 202.118.3.1/24 至 202.118.3.3/24 三个外网地址，内网地址为 192.168.1.0/24 网段，需要实现内网地址可以使用 202.118.3.1 和 202.118.3.2 两个地址访问外网。

图1-8 源 NAT 配置组网图



2. 配置步骤

(1) 按照组网图组网。

(2) 在导航栏中选择“策略配置 > 对象管理 > 地址对象 >地址对象”，单击<新建>按钮，进入地址对象配置页面，如图 1-9 所示。

图1-9 地址对象配置

点击<提交>按钮，提交配置。

(3) 在导航栏中选择“策略配置 > NAT 转换策略> 地址池”，单击<新建>按钮，进入创建地址池配置页面配置地址池对象，如图 1-10 所示。

图1-10 地址池对象配置

点击<提交>按钮，提交配置。

(4) 在导航栏中选择“策略配置 > NAT 转换策略 > 源 NAT”，单击<新建>按钮，进入源 NAT 配置页面配置源 NAT 转换，如图 1-11 所示。

图1-11 源 NAT 规则配置

点击<提交>按钮，提交配置。

3. 配置注意事项

- 外网 IP-network 需要配置到地址 202.118.3.1 和 202.118.3.2 的路由，保证网络可达。

4. 验证配置

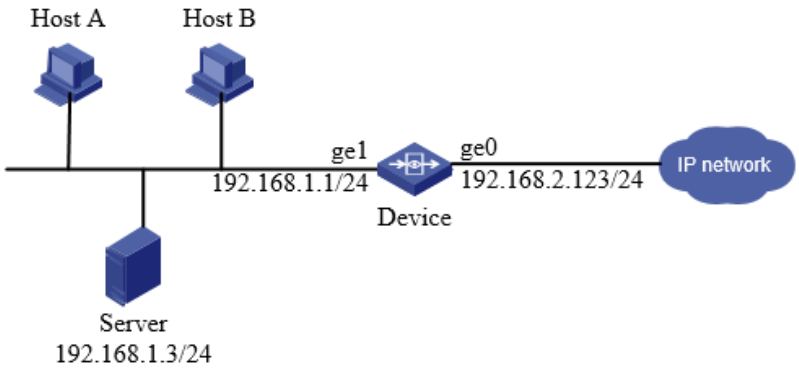
配置完成后，内网 PC 可以直接访问外网。

1.8.2 目的 NAT 配置案例

1. 组网需求

公司内网有一台服务器对外提供 HTTP 服务，内网地址为 192.168.1.3，服务端口为 TCP 80，对外开放的地址为 202.118.3.2，对外开放的服务端口为 TCP 8080，现需要在外网可以直接访问内网服务器。

图1-12 目的 NAT 配置组网图



2. 配置步骤

(1) 按照组网图组网

(2) 在导航栏中选择“策略配置 > 对象管理 > 地址对象>地址对象”，单击<新建>按钮，进入地址对象配置页面，如图 1-13 所示。

图1-13 地址对象配置

点击<提交>按钮，提交配置。

(3) 在导航栏中选择“策略配置 > NAT 转换策略 > 地址池”，单击<新建>按钮，进入创建地址池配置页面配置地址池对象，如图 1-14 所示。

图1-14 地址池对象配置

点击<提交>按钮，提交配置。

(4) 在导航栏中选择“策略配置 > 对象管理 > 服务对象> 自定义服务”，单击<新建>按钮，进入自定义服务配置页面配置服务对象，如图 1-15 所示。

图1-15 新建自定义服务

点击<提交>按钮，提交配置。

(5) 在导航栏中选择“策略配置 > NAT 转换策略 > 目的 NAT”，单击<新建>按钮，进入目的 NAT 配置页面配置目的 NAT 转换，如图 1-16 所示。

图1-16 目的 NAT 配置

3. 配置注意事项

- 外网 IP-network 需要配置到地址 202.118.3.2 的路由，保证网络可达。

4. 验证配置

配置完成后，外网可以访问内网服务器。

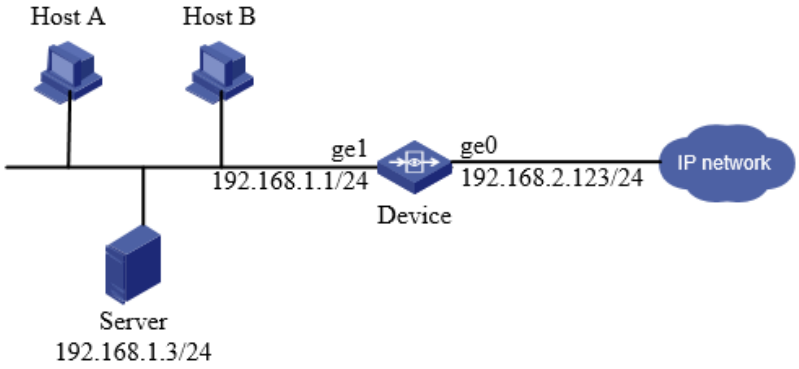
1.8.3 静态 NAT 配置案例

1. 组网需求

内网有一台服务器对外提供服务，服务器的内网地址为 192.168.1.3，映射的公网地址为 202.118.3.1。

2. 组网图

图1-17 静态 NAT 配置组网图



3. 配置步骤

(1) 按照组网图组网。

(2) 在导航栏中选择“策略配置 > NAT 转换策略 > 静态 NAT”，单击<新建>按钮，进入静态 NAT 配置页面，如图 1-18 所示。

图1-18 静态 NAT 配置

点击<提交>按钮，提交配置。

4. 配置注意事项

- 外网 IP-network 需要配置到地址 202.118.3.1 的路由，保证网络可达。

5. 验证配置

配置完成后，外网通过 IP 地址 202.118.3.1 可以访问内部服务器。

目 录

1 链路负载均衡 ····· 1-1
1.1 链路负载均衡简介 ····· 1-1
1.2 配置链路负载均衡 ····· 1-1
1.3 配置负载均衡出接口 ····· 1-3
1.4 配置免负载均衡地址 ····· 1-4
1.5 负载均衡策略配置 ····· 1-5
1.6 服务器负载均衡 ····· 1-6
1.7 服务器负载均衡配置 ····· 1-8
1.7.1 组网图形 ····· 1-8
1.7.2 组网需求 ····· 1-8
1.7.3 配置思路 ····· 1-8
1.7.4 操作步骤 ····· 1-9

1 链路负载均衡

1.1 链路负载均衡简介

信息时代，工作越来越离不开网络，为了规避运营商出口故障带来的网络可用性风险，和解决网络带宽不足带来的网络访问问题，企业往往会租用两个或多个运营商出口（如：电信、网通等）。如何合理运用多个运营商出口，既不造成资源浪费，又能很好的服务于企业，因而产生了多链路负载均衡的需求。传统的策略路由也可以在一定程度上解决该问题，但是策略路由配置不方便，而且不够灵活，无法动态适应网络结构变化，且策略路由无法根据带宽进行报文分发，造成高吞吐量的链路无法得到充分利用。负载均衡技术，通过动态算法，也能够在多条链路中进行负载均衡，算法配置简单，且具有自适应能力，能很好的解决上述问题。

本功能具有如下功能点：

- 根据实际配置，对加入到负载均衡，且路由可达的接口，做负载均衡。
- 根据实际配置，可实现基于带宽、优先级做负载均衡。
- 可配置带宽、阈值，当达到阈值后，可不再负载流量。
- 可配置过载保护接口，当负载均衡的所有接口都达到阈值后，流量走指定的接口。
- 可配置健康检查，检查每个负载均衡接口的连通状况。

说明

链路负载均衡目前最多可配置四个接口组，每个接口组下最多可配置四个接口。

1.2 配置链路负载均衡

通过界面“策略配置>负载均衡策略>链路负载均衡”，单击“新建”按钮，如图 1-1 所示，各配置项、接口配置项含义如表 1-1、表 1-2 所示。

图1-1 链路负载均衡配置界面

表1-1 链路负载均衡配置说明

参数	说明
名称	负载均衡组名称。
启用	启用或关闭负载均衡组。
负载均衡策略	负载均衡方式，基于带宽，基于优先级。
接口配置	向负载均衡组中添加负载均衡接口，只有路由的下一跳都在同一个负载均衡接口组时，才走负载均衡，否则按之前的路由策略走。

表1-2 接口配置项含义

参数	说明
接口名称	加入到负载均衡组的接口。
带宽	该接口对应的带宽，单位为MB，范围1-10000，该带宽不是接口物理带宽，而是从运营商购买的带宽，指的是下行带宽。
阈值	该接口的带宽限制，1-100%，由带宽乘以阈值比例，得出最后用于比较是否达到阈值的值，阈值是否达到，看到时候接口下的下行速率。
优先级	优先级可选范围1-4，数值越小越优先
作为过载保护接口	该接口是否作为过载保护接口，当所有接口都达到阈值后，流量将从过载报户口转发，若配置了多个过载保护口，将选择当前负载较低的接口使用，负载的计算公式为：下行速率/接口配置的下行带宽。

参数	说明
健康检查	通过引用对应的track条目，检查该接口的连通状况，当健康检查失败时，该接口将不再参与后续新建流量的转发，但之前已在该接口转发的流量，还将继续转发，直到流老化。
操作	可对接口配置进行编辑和删除。

1.3 配置负载均衡出接口

通过界面“策略配置>负载均衡策略>负载均衡出接口”，单击“新建”按钮，如图 1-2 所示，负载均衡出接口参数说明如表 1-3 所示。

图1-2 负载均衡出接口

表1-3 负载均衡出接口说明

参数	说明
出接口	选择出接口。

参数	说明
下一跳	路由选择的目的地址。
描述	出接口描述。
健康检查	开启或关闭健康检查功能。 名称：健康检查名称。 类型：支持ICMP类型。 检查地址：健康检查地址一般配置下一跳或下一条设备地址。 间隔：间隔x秒发送一次检查报文，不论是否成功，都会发送。 重试次数：重试次数M，表示已经有M次没有收到检查报文的回应之后，才会认为健康检查失败。 检查状态：显示此前检查状态。 新建：可新建健康检查项目配置。 操作：可删除健康检查项目配置。
DNS服务器	DNS服务器默认关闭，如果开启dns服务器功能，经过负载均衡的dns流量会进行dns转换。 手动配置：手动添加主DNS和备DNS 继承链路配置：继承链路出接口的DNS dns探测：开启关闭DNS探测功能 dns探测失败动作：DNS探测失败分两种，一种是禁用dns-dnat功能，另一种是禁用负载均衡出接口

1.4 配置免负载均衡地址

通过界面“策略配置>负载均衡策略>免负载均衡地址”，单击“设置”按钮，如图 1-3 所示，免负载均衡地址各项说明如表 1-4 所示。

图1-3 免负载均衡地址配置界面

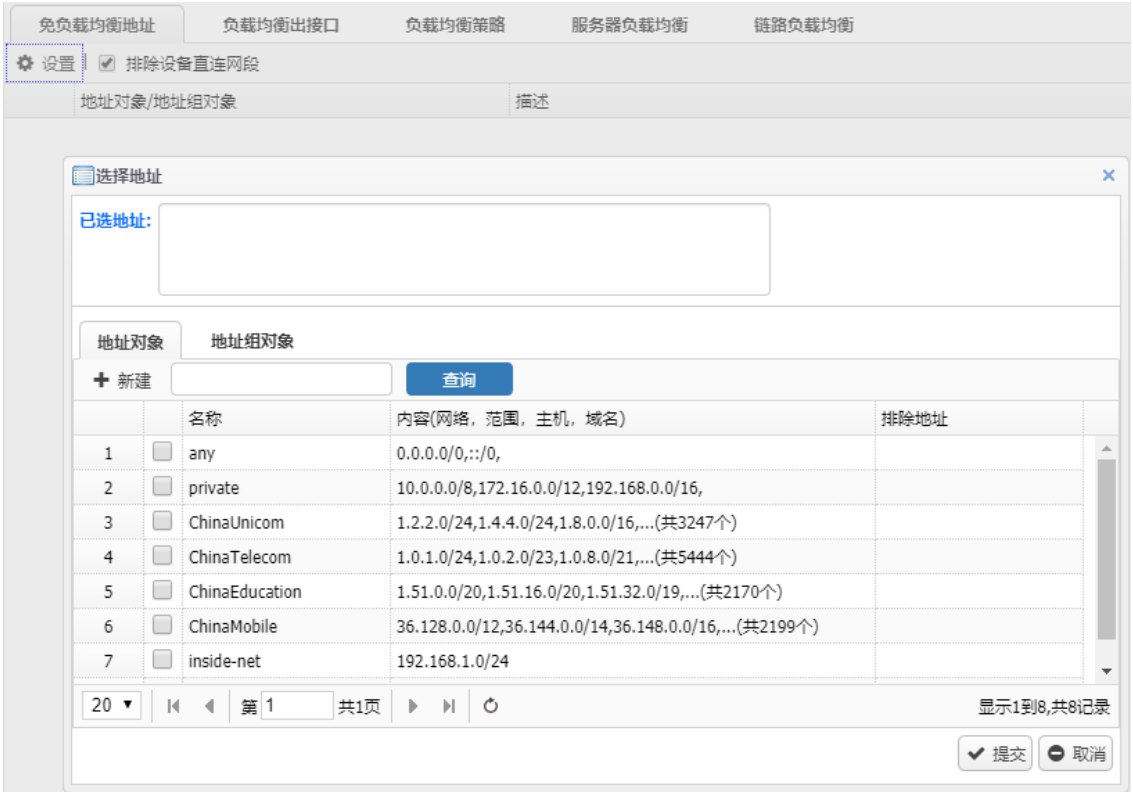


表1-4 免负载均衡说明

参数	说明
已选地址	选中的地址将不进入负载均衡流程。
新建	新建地址对象。
查询	查询地址对象或者地址组对象。
排除设备直连网段	设备的直连网段不进入负载均衡流程。

1.5 负载均衡策略配置

通过界面“策略配置>负载均衡策略>负载均衡策略”，单击“新建”按钮，如图 1-4 所示，负载均衡策略配置各项含义如表 1-5 所示。

图1-4 负载均衡策略界面

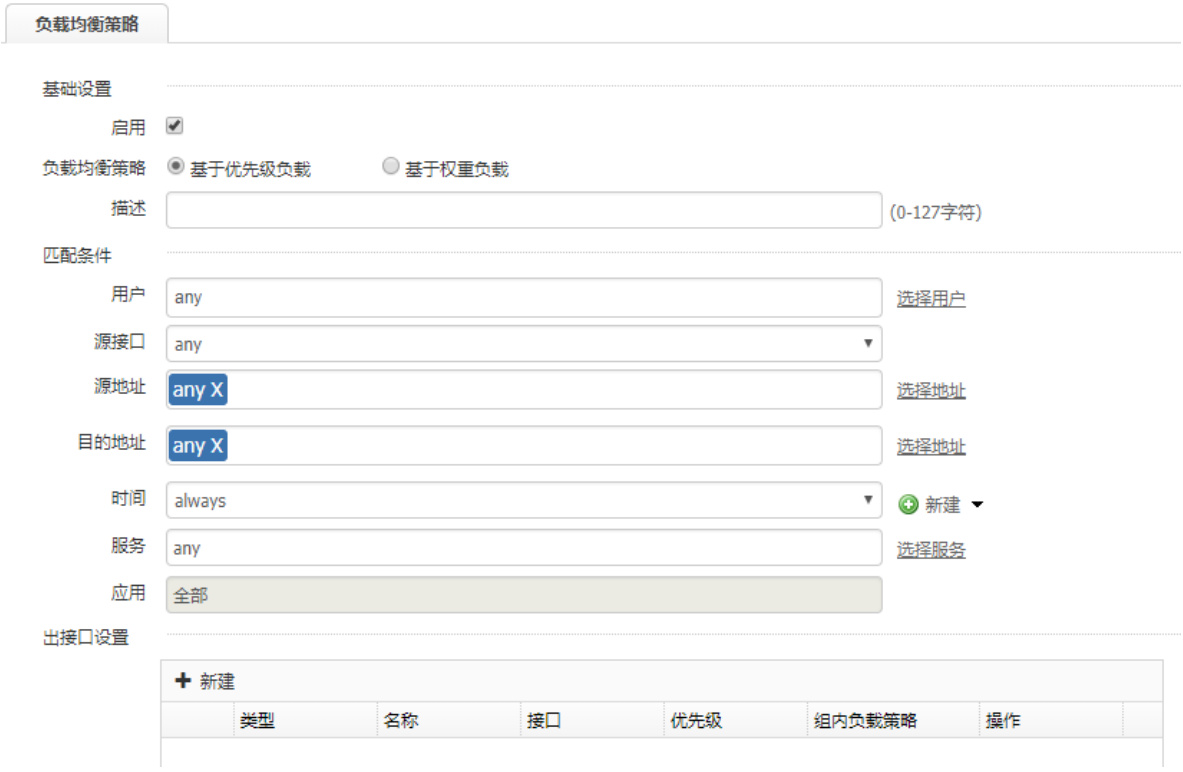


表1-5 负载均衡策略说明

参数	说明
启用	开启负载均衡策略。
负载均衡策略-基于优先级	多条链路在同一调度策略中，根据由上到下的优先级顺序将目标流量进行分发。
负载均衡策略-基于权重	多条链路在同一调度策略中，根据加权调度算法将目标流量根据权重比进行分发。
描述	负载均衡策略的描述。
匹配条件	完全匹配上用户，源接口，源地址，目的地址，时间，服务，应用，才能命中负载策略。

1.6 服务器负载均衡

进入页面“策略配置>负载均衡策略>服务器负载均衡”，单击“新建”按钮，如图 1-5 所示。

图1-5 服务器负载均衡策略页面

服务器负载均衡策略配置各项含义如表 1-6 所示。

表1-6 服务器负载均衡策略说明

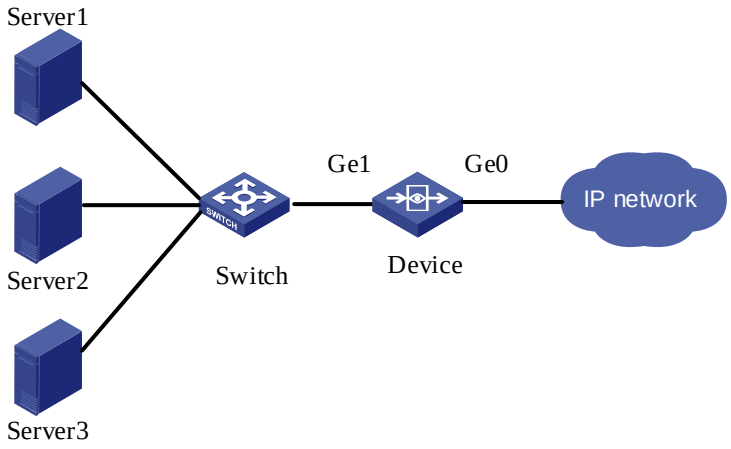
参数	说明
启用	开启关闭服务器负载均衡策略。
ID	服务器负载均衡策略ID值。
源地址	服务器负载均衡规则匹配的源地址，可引用地址节点或地址组。
目的地址	服务器负载均衡规则匹配的目的地址，可引用地址节点或地址组。
服务	服务器负载均衡策略规则匹配的服务名，可引用服务资源或服务组。
接口	服务器负载均衡策略规则匹配的入接口名。

参数	说明
转换类型	需要转换的类型，可选择地址映射、端口映射。 地址映射：只转换地址。 端口映射：转换地址和端口，选择该选项后，会有转换后端口需要填写。
服务器负载均衡算法	服务器负载均衡方式，基于源地址散列加权重分配或者基于基于权重分配，权重值在实服务器中进行配置。
实服务器	配置实服务器名、地址和权重三项。实服务器名为实服务器的名称。地址为实服务器的IP地址。权重为该实服务器在整个策略所占的权值。
服务器探测	配置服务器探测，探测类型可为ICMP探测或TCP探测。TCP探测为对对应的IP地址和端口号进行探测。

1.7 服务器负载均衡配置

1.7.1 组网图形

图1-6 服务器负载均衡组网



1.7.2 组网需求

公司内网有三台服务器对外提供 HTTP 服务，内网地址分别为 192.168.1.10、192.168.1.20、192.168.1.30，服务端口为 tcp 80，对外开放的地址为 202.118.3.2，对外开放的服务端口为 tcp 8080，现需要在外网可直接访问内网服务器，且能根据三台服务器的性能按权重提供服务。

1.7.3 配置思路

- 配置外网地址对象 VSIP，地址为 202.118.3.2。
- 配置端口为 8080 的自定义服务。
- 配置服务器负载均衡策略，需要配置策略 ID 号；源地址为 any；目的地址为外网地址对象 VSIP；服务为上述配置的自定义服务；接口选择 ge0；转换类型为端口映射，且端口为 80 端口；负

载均衡算法选择源地址散列+权重；新建 IP 地址分别为 192.168.1.10、192.168.1.20、192.168.1.30 的实服务器；开启探测，同时选择探测类型为 TCP。

1.7.4 操作步骤

(1) 按照图 1-6 组网图组网

(2) 在导航栏中选择“策略配置->对象管理->地址对象->IPv4 地址对象”，单击“新建”按钮，进入 IPv4 地址对象配置页面，如图 1-7 所示。配置完成后点击“提交”按钮，提交配置。

图1-7 地址对象配置

(3) 在导航栏中选择“策略配置->对象管理->服务对象->自定义服务”，单击“新建”按钮，进入自定义服务配置页面配置服务对象，如图 1-8 所示。配置完成后点击“提交”按钮，提交配置。

图1-8 自定义服务配置

(4) 在导航栏中选择“策略配置-> 负载均衡策略- >服务器负载均衡”，单击“新建”按钮，进入服务器负载均衡配置页面，如图 1-9 所示。配置完成后点击“提交”按钮，提交配置，如图 1-10。

图1-9 服务器负载均衡规则配置

图1-10 服务器负载均衡配置完成页面

目 录

1 DNS-DNAT ····· 1-1
1.1 DNS-DNAT 简介 ····· 1-1
1.2 NS-DNAT 配置 ····· 1-1
1.3 DNS-DNAT 典型配置举例 ····· 1-2
1.3.1 DNS-DNAT 典型配置举例 ····· 1-2

1 DNS-DNAT

1.1 DNS-DNAT简介

DNS-DNAT 的功能主要是在链路负载均衡策略的接口上设置 DNS 服务器的地址，同时在 DNS 的 request 的出接口上，我们将用户的 DNS 目的地址更换为接口上的 DNS 服务器的 IP 地址，从而保证从该链路上返回来的 IP 地址为该运营商提供的服务。

1.2 NS-DNAT配置

通过菜单“策略配置 > 负载均衡策略 > 负载均衡出接口”，点击<新建>进入负载均衡出接口新建页面，如图 1-1 所示。在该页面上，勾选 DNS 服务器的“开启”（默认 dns 服务器是关闭状态），即可以配置 dns 服务器。

图1-1 DNS 服务器配置

DNS 服务器各个配置项的含义如表 1-1 所示。

表1-1 DNS 服务器配置项含义

标题项	说明
DNS服务器的开启	开启DNS探测功能。
DNS服务器的关闭	关闭DNS探测功能。
手动配置	手动添加DNS地址。
继承配置	如果出接口是pppoe或者dhcp这种动态获取地址的出接口，DNS地址动态获取，不需要手动配置。
主备DNS地址	DNS流量转换后的dns地址。
DNS探测失败后动作—禁用DNS-DNAT功能	探测失败后，dns流量不进行dns-dnat转变。
DNS探测失败后动作—禁用负载均衡出接口	探测失败后，负载均衡出接口状态变成down，出接口不转发流量。

1.3 DNS-DNAT典型配置举例

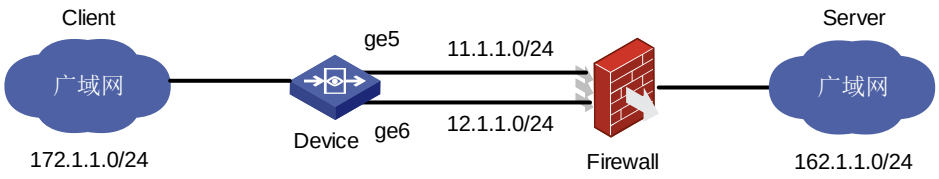
1.3.1 DNS-DNAT 典型配置举例

1. 组网需求

- 测试仪模拟 client 端地址（172.1.1.0/24），模拟 server 端地址（162.1.1.0/24）
- 设备有两个接口 ge4-0 和 ge4-1 与外网连通，并且这两个接口均可去往 server 端。
- DNS 服务器配置的主备 DNS 可以正常解析 www.baidu.com

2. 组网图

图1-2 DNS-dnat 组网图



3. 配置步骤

(1) 按照组网图组网。

如图所示，进入“策略配置 > 负载均衡策略 > 负载均衡出接口”，选择负载均衡出接口界面，查看负载均衡出接口配置，如图 1-3 所示。

图1-3 负载均衡出接口配置

点击<新建>，进入负载均衡出接口配置界面，配置完基础配置（基础配置参考《负载均衡》相关介绍）后，勾选 DNS 服务器对应的“开启”项（默认 dns 服务器是关闭状态），添加 DNS 服务器，如图 1-4、图 1-5 所示。

图1-4 添加 DNS 服务器配置 1

图1-5 添加 DNS 服务器配置 2

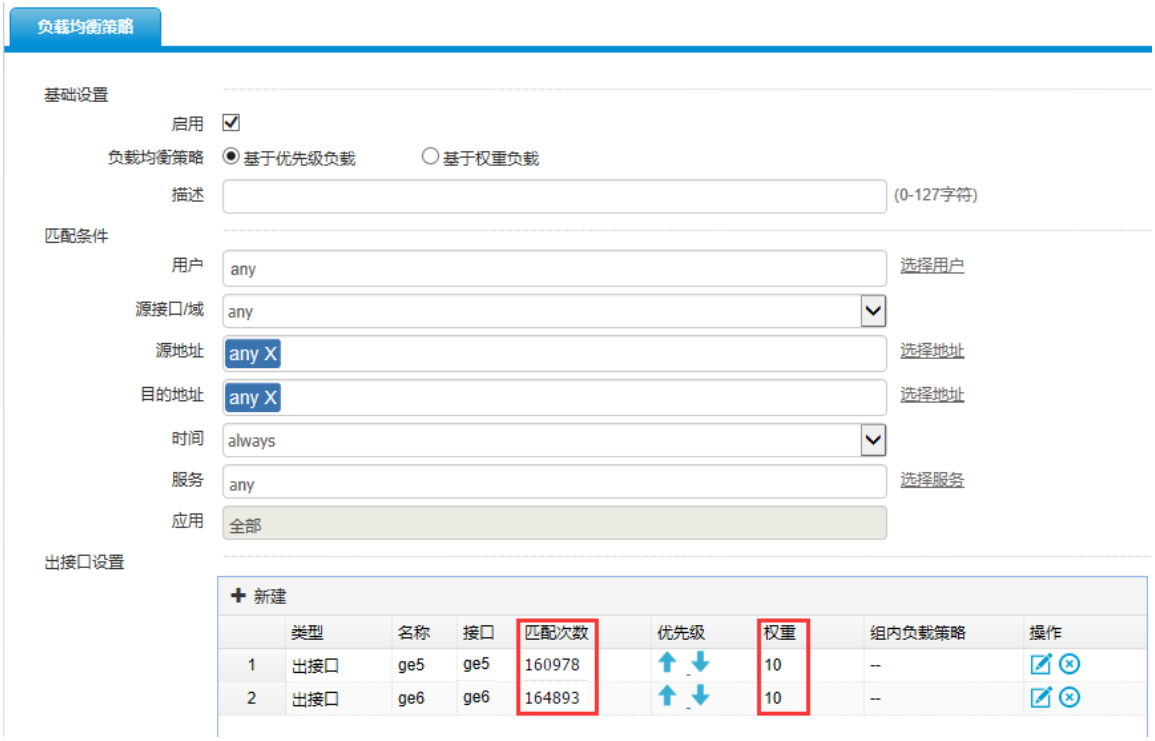
进入“策略配置 > 负载均衡策略”，选择“负载均衡策略”页面，点击<新建>，添加负载均衡策略配置，如图 1-6 所示。

图1-6 添加负载均衡配置

4. 验证配置

在 web 界面点击“负载均衡策略”，查看出接口的匹配次数（负载均衡策略权重，两个出接口权重相同，所以出接口的匹配次数几乎相同）

图1-7 查看出接口的匹配次数



查看 DNS 流量是否正常转换成设备配置 DNS 主地址：

```
host# display ip connection all
current connection count: 46
Protocol:    UDP State:Complete    PolicyID:1       VrfId:0
               Status: 0x0080080e                   FastCode: 0x80000207
               UserName: 172.1.1.33                 AppName: dns
               Expire: 00:00:28                     Existed: 00:00:36
               Source Dir: 172.1.1.33:62495      >  200.1.1.2:53             PKTS 1
               Reply  Dir: 162.1.1.2:53          >  172.1.1.33:62495         PKTS 1
               This connection has DST_NAT
Protocol:    UDP State:Complete    PolicyID:1       VrfId:0
               Status: 0x0080080e                   FastCode: 0x80000207
               UserName: 172.1.1.31                 AppName: dns
               Expire: 00:00:38                     Existed: 00:00:26
               Source Dir: 172.1.1.31:63493      >  200.1.1.2:53             PKTS 1
               Reply  Dir: 162.1.1.2:53          >  172.1.1.31:63493         PKTS 1
               This connection has DST_NAT
Protocol:    UDP State:Complete    PolicyID:1       VrfId:0
               Status: 0x0080080e                   FastCode: 0x80000207
               UserName: 172.1.1.37                 AppName: dns
               Expire: 00:01:02                     Existed: 00:00:02
               Source Dir: 172.1.1.37:1287       >  200.1.1.2:53             PKTS 1
               Reply  Dir: 162.1.1.2:53          >  172.1.1.37:1287       PKTS 1
               This connection has DST_NAT
```

说明

DNS-DNAT 的默认 dns 健康检查地址是 www.baidu.com。

DNS 使用主备 DNS 地址进行探测，10s 一次，如果三次探测不成功，设备认为 DNS 地址不可用

如果设备配置的主备 DNS 地址均正常可用，默认使用主 DNS 地址，当主 DNS 地址不可用，在使用备 DNS 地址

目 录

1 流控策略 ····· 1-1
1.1 流控策略概述 ····· 1-1
1.2 线路 ····· 1-2
1.3 通道 ····· 1-3
1.4 限制通道 ····· 1-5
1.5 惩罚通道 ····· 1-7
1.6 排除策略 ····· 1-8
1.7 流量监控 ····· 1-9
1.8 配置举例 ····· 1-9
1.8.1 流控策略配置案例 ····· 1-9
1.8.2 排除策略配置案例 ····· 1-13

1 流控策略

1.1 流控策略概述

流控策略是通过流量分析，对各种网络流量进行精细控制和调度的一种方法。

流控策略具有如下特点：

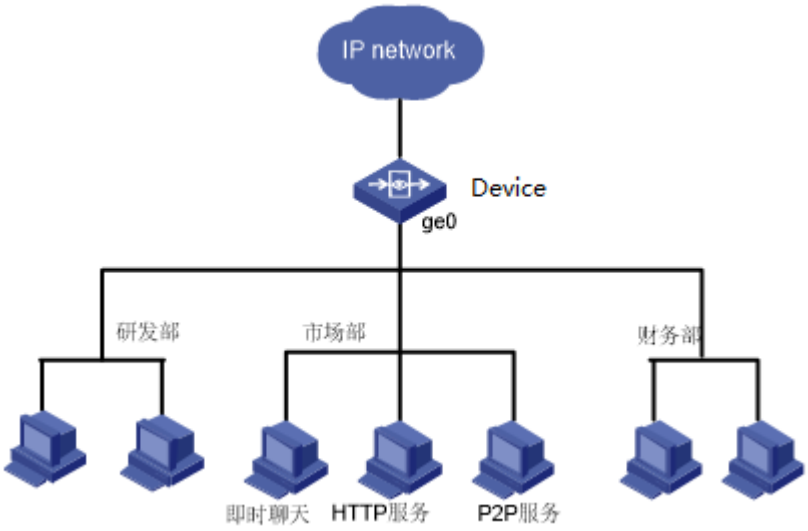
- 使用线路和通道，实现层次化的流控策略。
- 支持保障带宽和最大带宽。
- 支持弹性带宽或带宽借用，充分利用网络资源。
- 能够根据应用、服务、用户、地址对象等进行流量控制。
- 支持优先级，确保高优先级的应用能够获得带宽。
- 支持按 IP 及用户进行流量限速。
- 流控策略可以在指定的时间内生效。
- 流量监控可以查看各线路及通道当前流量速率。

流控策略涉及的概念解释如表 1-1 所示：

表1-1 流控策略概念表

概念	解释
线路	一般和一个物理接口对应，说明数据流量从哪个接口出或入，才匹配该线路。
通道	根据应用、服务、用户、地址对象等，虚拟的控制带宽单元的概念。
限制通道	根据接口、应用、服务、用户、地址对象等进行带宽限制的通道。
惩罚通道	当用户接入网络超过指定的时长或流量限额时进行惩罚的通道，只能在限额策略中引用。
保障带宽	当网络繁忙的时候，需要保证使用的带宽。
最大带宽	当网络空闲的时候，能够最大使用的带宽。
默认通道	未匹配用户指定通道的流量，按照默认通道进行流量控制。

图1-1 流控策略工作原理示意图



- ge0 接口上行带宽为 10M，市场部、财务部和研发部共享 10M 带宽，其中市场部的保障带宽为 6M，研发部为 4M，财务部保障带宽为 0M。
- 即时聊天优先级最高，HTTP 服务优先级次之，P2P 服务优先级最低。
- 当研发部和市场部都在使用带宽的时候，市场部和研发部的保障带宽分别为 6M 和 4M。
- 如果研发部和财务部不使用带宽，则市场部可以充分使用 10M 带宽资源。
- 即时聊天有较高优先级、P2P 有较低优先级，因此即使 P2P 流量很大，也不会导致即时聊天丢包。

1.2 线路

在导航栏中选择“策略配置 > 流量控制策略 > 流量控制”，单击<新建>按钮，选择<线路>进入线路设置配置页面，如图 1-2 所示。线路设置详细配置说明，如表 1-2 所示。

图1-2 线路设置页面

表1-2 线路设置详细配置

标题项	说明
启用	是否启用线路规则。
名称	线路名称。
绑定接口	线路绑定的接口，一个接口仅能够和一个线路绑定。
带宽管理（出）	配置接口出方向带宽，单位可以选择Kb/Mb/Gb。
带宽管理（入）	配置接口入方向带宽，单位可以选择Kb/Mb/Gb。
带宽管理（出和入）的启用	是否启用接口出方向或入方向的带宽管理。

说明

- 线路的出方向带宽是指该接口发送报文方向的带宽。
- 线路的入方向带宽是指该接口接收报文方向的带宽。

1.3 通道

在导航栏中选择“策略配置 > 流量控制策略> 流量控制”，单击<新建>按钮，选择<通道>进入通道配置页面，如图 1-3 所示。通道详细配置说明，如表 1-3 所示。

图1-3 通道配置页面

表1-3 通道详细配置

标题项	说明
启用	启用通道。
名称	通道的名称。
上一级	父通道或线路。
级别	通道的优先级，优先级高的通道，就有更多可能借用上级父通道的带宽，共有高、中、低三个优先级级别。
最大带宽（出）	该通道的上行最大带宽，不能大于其上级通道的带宽，支持百分比配置，当线路带宽改变后，该带宽也会按百分比自动做相应调整。

标题项	说明
上行保障带宽	通道的上行最大保障带宽，不能大于其上级通道的保障带宽。支持百分比配置，当线路带宽改变后，该带宽也会按百分比自动做相应调整。
最大带宽（入）	该通道的下行最大带宽，不能大于其上级通道的带宽。支持百分比配置，当线路带宽改变后，该带宽也会按百分比自动做相应调整。
下行保障带宽	通道的下行最大保障带宽，不能大于其上级通道的保障带宽。支持百分比配置，当线路带宽改变后，该带宽也会按百分比自动做相应调整。
每终端限速配置	选择限速的对象： 每IP限速：根据IP地址进行限速。 每用户限速：根据用户名进行限速。
出	每终端流量限制的上行流量的最大带宽。
入	每终端流量限制的下行流量的最大带宽。
匹配用户/组	流量控制匹配的用户对象或用户组名称。
匹配应用	流量控制匹配的应用对象名称。
服务	流量控制匹配的服务对象名称。
地址	流量控制匹配的地址对象。
终端型号	选择终端型号，默认为any。此功能依赖于第三方用户同步中的ddi终端用户功能，需要将终端型号信息同步给设备。
时间	流量控制匹配的时间对象。

1.4 限制通道

在导航栏中选择“策略配置 > 流量控制策略 > 流量控制”，单击<新建>按钮，选择<限制通道>进入限制通道配置页面，如图 1-4 所示。限制通道详细配置说明，如表 1-4 所示。

图1-4 限制通道

表1-4 限制通道详细配置

标题项	说明
启用	启用限制通道。
名称	限制通道的名称。
带宽设定	设定限制通道的总带宽。
出	限制通道上行流量总带宽。
入	限制通道下行流量总带宽。
每终端限速配置	选择限速的对象： 每IP限速：根据IP地址进行限速。 每用户限速：根据用户名进行限速。

标题项	说明
出	每终端流量限制的上行流量的最大带宽。
入	每终端流量限制的下行流量的最大带宽。
接口	限制通道绑定的接口。
匹配用户/组	流量控制匹配的用户对象或用户组名称。
匹配应用	流量控制匹配的应用对象名称。
服务	流量控制匹配的服务对象名称。
地址	流量控制匹配的地址对象。
时间	流量控制匹配的时间对象。

说明

限制通道是实现带宽限速的通道，不依赖于线路，可以直接绑定接口，且限制通道匹配优先级高于通道优先级。

1.5 惩罚通道

在导航栏中选择“策略配置 > 流量控制策略 > 流量控制”，单击<新建>按钮，选择<惩罚通道>进入惩罚通道配置页面，如图 1-5 所示。惩罚通道详细配置说明，如表 1-5 所示。

图1-5 惩罚通道

表1-5 惩罚通道详细配置

标题项	说明
名称	限制通道的名称。
带宽设定	设定惩罚通道的总带宽。
出	惩罚通道上行流量总带宽。
入	惩罚通道下行流量总带宽。
每终端限速配置	选择限速的对象： 每IP限速：根据IP地址进行限速。 每用户限速：根据用户名进行限速。
出	每终端流量限制的上行流量的最大带宽。
入	每终端流量限制的下行流量的最大带宽。

说明

惩罚通道是实现当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，不依赖于线路，也不依赖于接口，只能被限额策略引用，当用户达到限额阈值时才会进入相应的惩罚通道。

1.6 排除策略

在导航栏中选择“策略配置 > 流量控制策略 > 排除策略”，单击<新建>按钮进入排除策略配置页面，如图 1-6 所示。排除策略详细配置说明，如表 1-6 所示。

图1-6 排除策略

表1-6 排除策略详细配置

标题项	说明
用户	用户或用户组对象，点击“选择用户”会弹出用户选择框。

标题项	说明
地址	地址或地址组对象。

1.7 流量监控

在导航栏中选择“策略配置 > 流量控制策略 >流量监控”，可以查看各线路、通道、限制通道以及惩罚通道当前流量速率，如图 1-7 所示。

图1-7 流量监控

1.8 配置举例

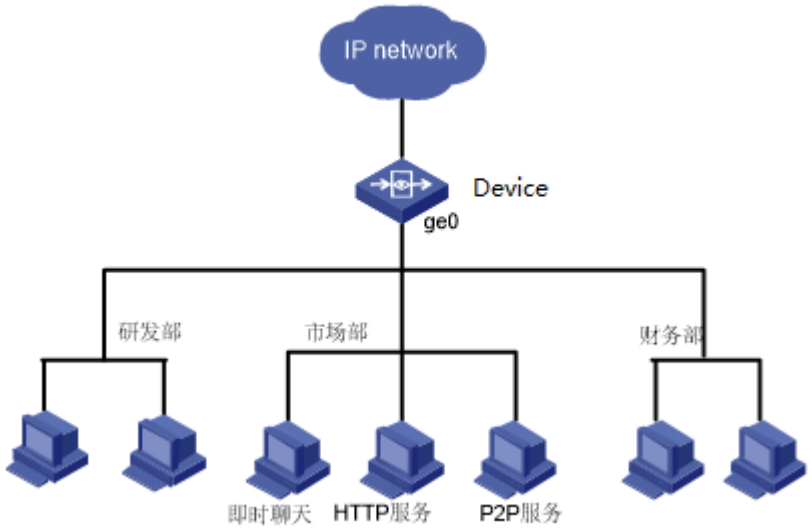
1.8.1 流控策略配置案例

1. 组网需求

P2P 类型的访问流量一般都会很大，会占用大量的公司带宽，导致实时性要求比较高的服务可能会出现延时或丢包，所以需要限制 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，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 6M。

2. 组网图

图1-8 流控策略配置组网图



3. 配置步骤

(1) 在导航栏中选择“策略配置 > 流量控制策略 > 流量控制 ”，单击<新建>按钮，选择<线路>进入线路设置配置页面，如图 1-9 所示。

图1-9 线路设置

点击<提交>按钮，提交配置。

(2) 创建研发部带宽保障策略，在导航栏中选择“策略配置 > 流量控制策略 > 流量控制”，单击<新建>按钮，选择<通道>进入通道配置页面，如图 1-10 所示。

图1-10 带宽保障策略配置

点击<提交>按钮，提交配置。

(3) 创建 P2P 带宽限制策略，在导航栏中选择“策略配置 > 流量控制策略 > 流量控制”，单击<新建>按钮，选择<限制通道>进入限制通道配置页面，如图 1-11 所示。

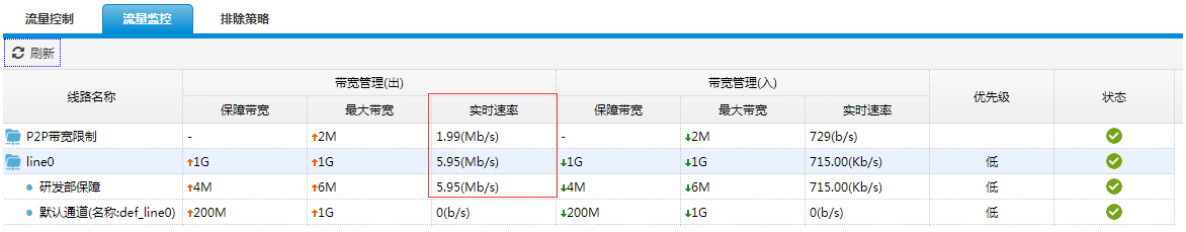
图1-11 P2P 带宽限制配置

点击<提交>按钮，提交配置。

4. 验证配置

配置完成后，在流量监控页面查看，确认 P2P 访问的最大流量为 2M，研发部流量为 4M-6M 之间。如图 1-12 所示。

图1-12 流量监控



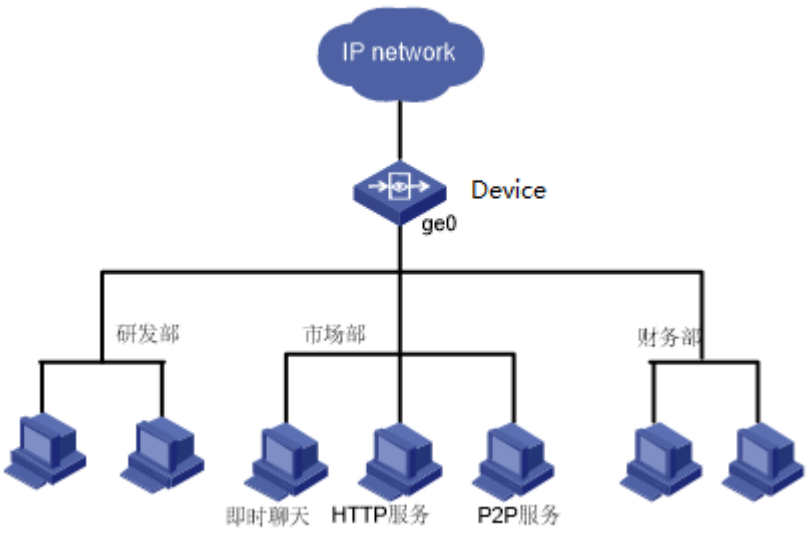
1.8.2 排除策略配置案例

1. 组网需求

要求公司研发部拥有访问外网优先权，不受流控策略控制。公司研发部的 IP 地址是 192.168.1.0/24 网段。

2. 组网图

图1-13 流控策略配置组网图



3. 配置步骤

(1) 在导航栏中选择“策略配置> 对象管理 > 地址 >IPv4 地址对象”，单击<新建>按钮，进入 IPv4 地址对象置配置页面，如图 1-14 所示。

图1-14 地址对象

点击<提交>按钮，提交配置。

(2) 在导航栏中选择“策略配置 > 流量控制策略 > 排除策略”，单击<新建>按钮，进入排除策略配置页面，如图 1-15 所示。

图1-15 排除策略

点击<提交>按钮，提交配置。

4. 验证配置

配置完成后，在流量监控页面查看统计，确认针对研发的 PC 不受流量控制策略的限制。如图 1-16 所示。

图1-16 流量监控

目 录

1 限额策略 ····· 1-1
1.1 限额策略概述 ····· 1-1
1.2 限额策略 ····· 1-1
1.3 限额用户统计 ····· 1-3
1.4 配置举例 ····· 1-4
1.4.1 限额策略配置案例 ····· 1-4

1 限额策略

1.1 限额策略概述

限额策略能够实现通过监控用户的上网时长或流量大小，在达到监控阈值后对用户进行惩罚限速或禁止上网，例如当用户当天使用的流控超过 500MB 的时候，才进行惩罚限速。这样的好处是，用户不超过日（月）限额的情况下，可以自由的使用网络带宽。当超过的时候，通过惩罚通道，能够让用户进入到一个较为低速通道里。

限额策略具有如下特点：

- 流量限额：支持日限额和月限额。
- 时长限额：支持日限额和月限额 。
- 支持设置惩罚时长。
- 支持提醒：达到限额条件后推送提醒页面提示用户，可以设置只提醒一次或定期提醒。
- 支持惩罚通道限速：基于时长惩罚或一直惩罚。
- 支持禁止上网：基于时长禁止上网或一直禁止上网。
- 支持限额统计：基于 IP 维度和用户账号维度。

1.2 限额策略

在导航栏中选择“策略配置 > 用户限额策略 > 限额策略”，单击“新建”进入限额策略配置界面，如图 1-1 所示。限额策略详细配置说明，如表 1-1 所示。

图1-1 配置限额策略

表1-1 限额策略详细配置

标题项	说明
启用	勾选后则启用限额策略。

标题项	说明
日志	勾选后记录日志。
名称	限额策略的名称。
描述	限额策略的描述信息。
用户	选择限额策略匹配的用户。
源地址	选择限额策略匹配的源地址。
目的地址	选择限额策略匹配的目的地址。
时间	选择限额策略匹配的时间对象。
应用	选择限额策略匹配的应用对象。
限额类型	可以选择流量限额或时长限额两种方式。
日限额	配置日限额额度。
月限额	配置月限额额度。
提醒设置	设置提醒功能开启以及提醒阈值、间隔。
启用	启用提醒设置。
阈值	提醒阈值设置，达到提醒阈值后会推送提醒页面。
间隔	提醒间隔设置，范围0-1440分钟，为0时代表只提醒一次。
惩罚设置	设置惩罚功能开启以及惩罚方式。
启用	启用惩罚功能
惩罚时长	惩罚时长设置，范围0-1200分钟，为0时代表一直惩罚。
添加到流控通道	设置惩罚通道，达到限额阈值后会匹配引用的惩罚通道。
禁止上网	惩罚动作为禁止上网。

1.3 限额用户统计

在导航栏中选择“策略配置 > 用户限额策略 > 限额用户统计”，可以查看限额用户流量或在线时长统计情况，如图 1-2 所示。限额用户统计详细说明，如表 1-2 所示。

图1-2 限额用户统计

表1-2 限额用户统计详细说明

标题项	说明
用户	显示用户账号或用户IP。
策略名	匹配的限额策略名称。
流量额度丨时长	限额策略中配置的流量阈值或时长阈值，包含日限额和月限额。
实际流量统计丨在线时长	当前实时流量或在线时长的统计，包含日限额和月限额。
网络访问状态	当前用户网络访问状态，包含禁止上网、限速、正常上网。

1.4 配置举例

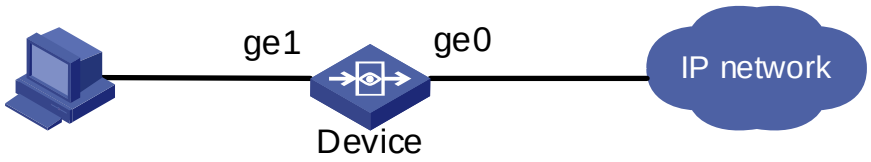
1.4.1 限额策略配置案例

1. 组网需求

针对内网用户上网流量每日限额 100M，未超过 100M 时可以自由使用网络，当日使用流量超过 100M 后，进行每 IP 惩罚限速 1M。

2. 组网图

图1-3 限额策略组网图



3. 配置步骤

(1) 创建惩罚通道，在导航栏中选择“策略配置 > 流量控制策略 > 流量控制 ”，单击<新建>按钮，选择<惩罚通道>进入惩罚通道配置页面，如图 1-4 所示。

图1-4 惩罚通道配置

点击<提交>按钮，提交配置。

(2) 创建限额策略，在导航栏中选择“策略配置 > 用户限额策略”，单击<新建>按钮，进入限额策略配置页面，如图 1-5 所示。

图1-5 限额策略配置

点击<提交>按钮，提交配置。

4. 验证配置

配置完成后，同时模拟 2 个用户上网，在流量监控页面查看，用户总流量为 2M。在限额用户统计页面显示用户为限速状态。如图 1-6、图 1-7 所示。

图1-6 流量监控

图1-7 限额用户统计

目 录

1 SSL 解密策略 ····· 1-1
1.1 概述 ····· 1-1
1.2 原理描述 ····· 1-1
1.2.1 基本原理 ····· 1-1
1.2.2 解密策略 ····· 1-1
1.2.3 过滤条件 ····· 1-2
1.2.4 证书管理 ····· 1-2
1.3 解密类型 ····· 1-2
1.3.1 HTTPS 解密 ····· 1-2
1.3.2 邮箱解密 ····· 1-3
1.4 解密策略例外功能 ····· 1-3
1.5 解密策略的应用 ····· 1-3
1.6 配置解密策略 ····· 1-3
1.6.1 配置 HTTPS 对象 ····· 1-3
1.6.2 生成 CA 证书 ····· 1-5
1.6.3 本地证书导入 ····· 1-7
1.6.4 配置解密策略 ····· 1-7
1.6.5 配置审计策略 ····· 1-8
1.7 配置 SSL 证书推送 ····· 1-11
1.7.1 启用 SSL 证书推送 ····· 1-11
1.7.2 修改 SSL 证书推送 ····· 1-11
1.7.3 禁用 SSL 证书推送 ····· 1-12
1.7.4 使用限制 ····· 1-13
1.8 配置举例 ····· 1-13
1.8.1 解密策略配置案例 ····· 1-13
1.8.2 SSL 证书推送典型配置举例 ····· 1-18

1 SSL 解密策略

1.1 概述

随着市场网络安全的发展，越来越多的客户将原有的 http 业务逐步的迁移到 https 上，这样很大程度上保证了客户访问网络的安全，数据不会轻易的被第三方窥视。这样网络管理员很大程度上，很难得到内网用户访问外网的相关数据。对企业，集团内网有很大的风险。基于此客户对行为管理产品的厂商提出要求，需要设备能够解密客户 https 的流量，从而完成对原有 https 流量的审计功能。

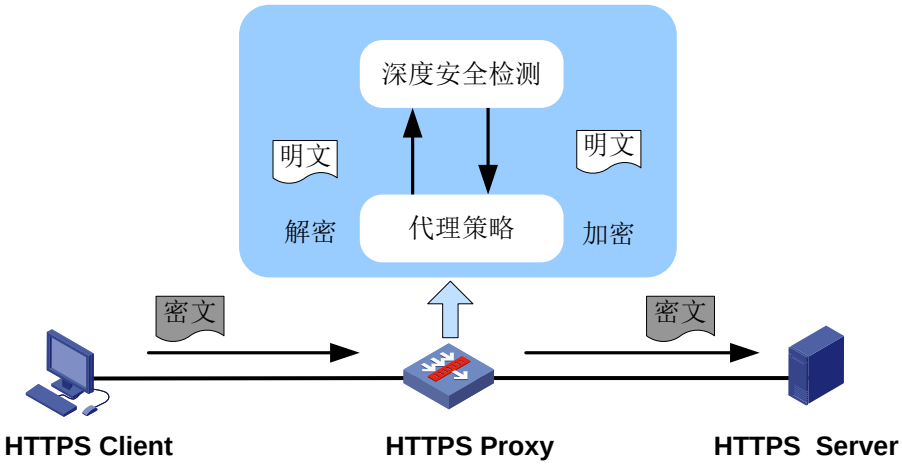
解密策略对设备的入接口、源 IP、目的 IP、https 对象进行访问控制，主要是对使用 SSL 协议传输的流量做审计，支持 HTTPS、邮箱类审计功能，并产生审计日志。

1.2 原理描述

1.2.1 基本原理

由于 SSL 流量是加密传输的，设备无法对加密的数据进行深度安全检测、审计等。所以 HTTPS 解密的本质就是对通过设备的报文进行 SSL 代理，本设备可通过配置解密策略来实现对所需要的流量进行 SSL 代理。

图1-1 SSL 代理功能示意图



如上图所示，设备将与解密策略过滤条件匹配成功的报文进行 SSL 代理，即分别与客户端和服务器建立 SSL 连接，然后对传输的报文先进行解密，再进行深度安全检测或者审计。完成流量审计后，对放行的报文重新进行加密，并发送到目的服务器。

1.2.2 解密策略

一个解密策略基本由过滤条件（包括入接口、源地址、目的地址等）和解密类型（即解密的对象）两部分组成，设备只会对于符合过滤条件的流进行解密。

设备上可以配置多条解密策略，其按照配置顺序从上到下进行匹配，当报文与某条策略匹配成功后，则根据此条解密策略进行报文解密，不再进行后续解密策略的匹配。基于以上的匹配原则，配置解密策略时建议按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。

1.2.3 过滤条件

设备支持的过滤条件包括：入接口、源地址、目的地址和 HTTPS 对象。其中 HTTPS 对象过滤条件仅支持在 HTTPS 解密类型中进行配置。一个解密策略中过滤条件之间是与的关系。

1.2.4 证书管理

实现 SSL 代理的本质就是通过设备在 Client 和 Server 之间进行证书管理。通过证书管理设备可以分别与 Client 和 Server 建立 SSL 连接，从而对数据进行解密。

使用设备自带的证书签发功能，或支持导入第三方证书，并被解密策略引用生效。用户证书一旦被解密策略引用，在证书过期之前，策略中包含的其它域名即可顺利的完成浏览。

- 设备自身支持证书签发的能力，可以为 ipsecvpn，https 解密等功能签发相关证书。
- 支持证书导入导出的功能，方便证书的管理，并且可导入第三方证书。解密策略在用户证书中选取一个证书使用，且支持证书之间的切换，证书被其它模块引用时仍可被解密策略引用。
- 支持 SSL 证书推送，可以实现 CA 证书安装检测，对指定用户进行 CA 证书下载页面的推送，终端用户可以在推送页面直接下载证书及安装指导。

1.3 解密类型

目前此功能支持的解密类型有 HTTPS 流量和邮箱流量。

1.3.1 HTTPS 解密

配置此种解密类型时，需要保证客户端的 DNS 报文经过设备，解密策略才能正常匹配生效，若 DNS 报文不经过设备的话，由于获取不到域名与 IP 的对应关系，这样经过设备的 https 域名站点的报文的目的 IP 与配置的 HTTPS 对象中域名解析的 IP 匹配不上，无法进入到解密流程从而也就无法解密。

系统内置的站点支持 https 解密功能，目前系统提供 128 个常见的站点域名，并且客户可以根据自己的需要自定义 10 个域名。

系统自带的站点格式举例：

- www.baidu.com
- www.taobao.com
- www.jd.com
- www.sogou.com
- www.so.com
- www.taobao.com
- www.amazon.cn

1.3.2 邮箱解密

该功能目前只针对如下常见邮箱提供解密：QQ（个人，企业），网易（163/126），标准的 pop3（995）、imap（993）和 smtp（465）同时开启 ssl 加密的邮箱。

当设备只需要进行邮箱解密，而不需要 HTTPS 流量解密时，不需要 DNS 流量经过设备。

1.4 解密策略例外功能

解密功能提供特定站点排除功能以及源地址排除的功能，针对排除的地址和站点不做 https 的解密，两者之间是或的关系，只要一个满足即排除不做解密，源地址排除功能使用地址对象配置。

1.5 解密策略的应用

解密的结果是为了可以对报文中的数据进行审计：

- 符合解密策略的数据全部上送审计模块完成审计，上送审计模块的全部是完成解密的明文数据。
- 符合解密策略的邮件，全部上送到审计模块，在完成审计的同时还支持基于关键字的过滤功能。保证内网用户的绝密信息不外泄。

1.6 配置解密策略

1.6.1 配置 HTTPS 对象

在导航栏中选择“策略配置>对象管理>URL>HTTPS 对象”进入 HTTPS 对象显示界面，如图 1-2 所示。

图1-2 HTTPS 对象显示界面

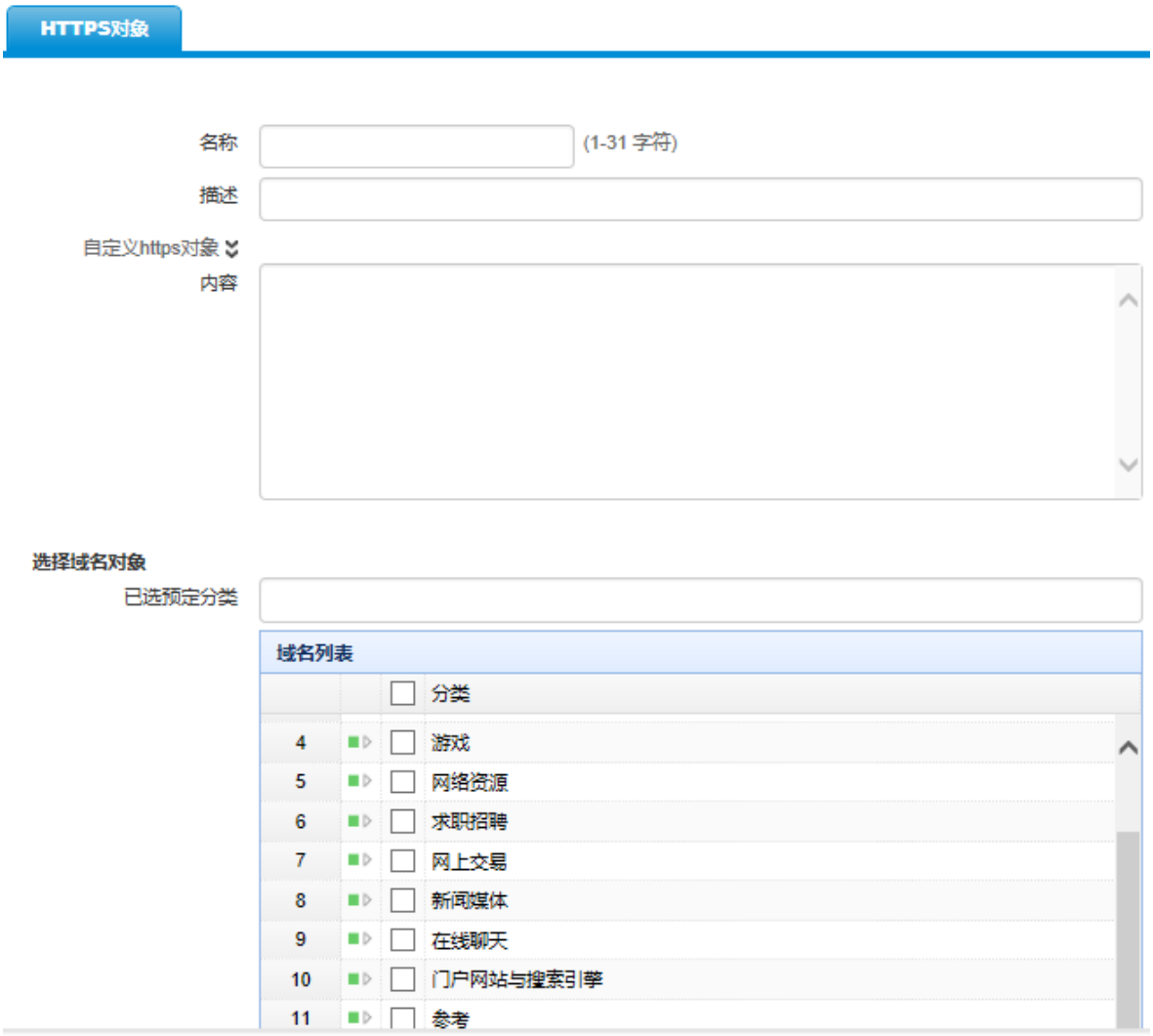
HTTPS 对象的含义如表 1-1 所示。

表1-1 HTTPS 对象显示信息描述表

参数	说明
新建	新建显示信息描述表
删除	删除显示信息描述表
编辑	编辑显示信息描述表

单击<新建>按钮，进入 HTTPS 对象配置界面，如图 1-3 所示。

图1-3 HTTPS 对象配置界面



HTTPS 对象详细配置说明，如表 1-2 所示。

表1-2 HTTPS 对象策略详细配置

参数	说明
名称	名称
描述	描述
自定义https对象	自定义https域名对象
已选预定分类	预定义的HTTPS域名对象

1.6.2 生成 CA 证书

在导航栏中选择“策略配置>对象管理>CA 服务器>根 CA 配置管理”，进入本地证书显示界面，如图 1-4 所示。

图1-4 根 CA 配置管理显示界面

根证书管理界面详细说明，如表 1-3 所示。

表1-3 根 CA 管理界面详细

参数	说明
生成CA根证书	生成CA根证书，为解密策略进行服务
导入CA根证书	导入CA根证书，此CA证书可以是设备上生成的，也可以是从外部CA证书导入的
导出CA根证书	导出CA根证书，可以为其它设备使用

单击“生成 CA 根证书”，进入生成 CA 根证书界面，如图 1-5 所示。

图1-5 生成 CA 根证书

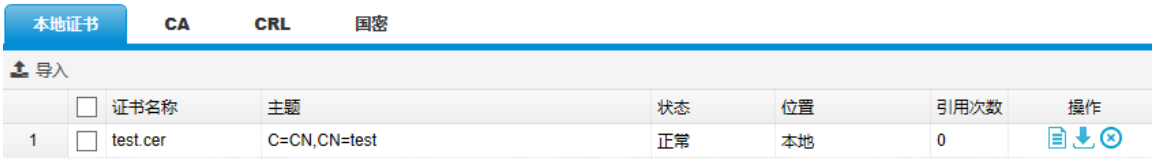
表1-4 生成 CA 证书详细说明

参数	说明
证书名称	证书名称
可选信息	详细信息
有效期	CA证书的有效期
密码	CA证书的秘钥
秘钥大小	秘钥大小（bit）

1.6.3 本地证书导入

在导航栏中选择“策略配置>对象管理>本地证书>证书>本地证书”，进入本地证书显示界面，如图1-6所示。

图1-6 本地证书显示界面



本地证书详细配置说明，如表 1-5所示。

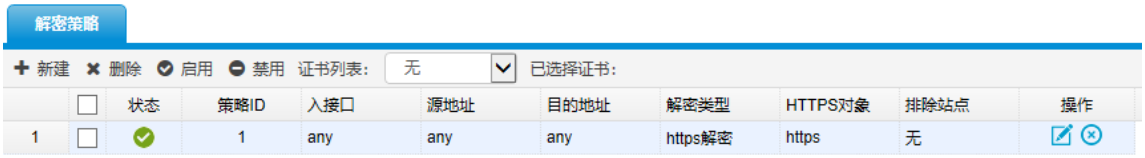
表1-5 本地证书优先级详细配置

参数	说明
导入	导入证书
详细信息	证书详细信息
导出	导出证书
删除	删除证书

1.6.4 配置解密策略

在导航栏中选择“策略配置>SSL 解密策略”，进入解密策略显示界面，如图 1-7所示。

图1-7 解密策略显示界面



解密策略配置详细说明，如表 1-6所示。

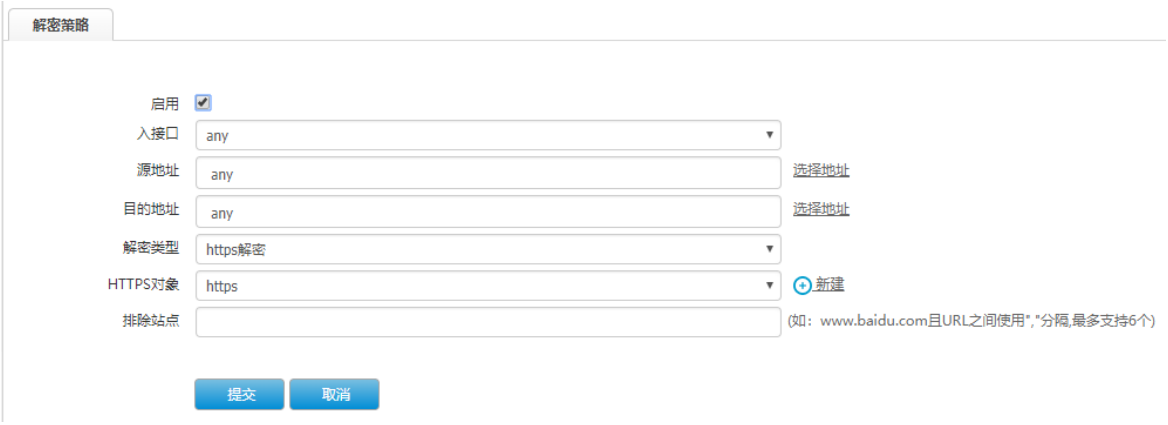
表1-6 解密策略显示详细

参数	说明
新建	新建解密策略
删除	删除解密策略
启用	启用解密策略
禁用	禁用解密策略

参数	说明
证书列表	选择引用证书，解密功能作为HTTPS代理，设备作为服务端需要此证书用来和客户端做SSL握手，为通信数据加解密
编辑	编辑解密策略
删除	删除解密策略

单击<新建>按钮，进入解密策略配置界面，如图 1-8 所示。

图1-8 解密策略配置界面



解密策略详细配置说明，如表 1-7 所示。

表1-7 解密策略详细配置

参数	说明
启用	启用解密策略
入接口	匹配入接口，表示从此接口收到的流量才会进行HTTPS解密
源地址	匹配解密策略的源地址，表示符合此源地址的流量才会进行HTTPS解密
目的地址	匹配解密策略的目的地址，表示符合此目的地址的流量才会进行HTTPS解密
解密类型	选择https解密或邮箱解密
HTTPS对象	只有匹配此HTTPS对象中域名的流量，才进行HTTPS解密。
排除站点	排除的站点不进行审计

1.6.5 配置审计策略

设备上可以配置多条审计策略，其按照配置顺序从上到下进行匹配，当报文与某条策略匹配成功后，则根据此条解密策略进行报文解密，不再进行后续解密策略的匹配。基于以上的匹配原则，配置解密策略时建议按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。

审计策略过滤条件之间是与的关系。

通过菜单“策略配置 > 审计策略”，进入审计策略显示页面。

单击<新建>按钮，进入审计策略配置页面，如图 1-9、图 1-10、图 1-11 所示。

图1-9 审计策略详细配置页面 1-基础配置

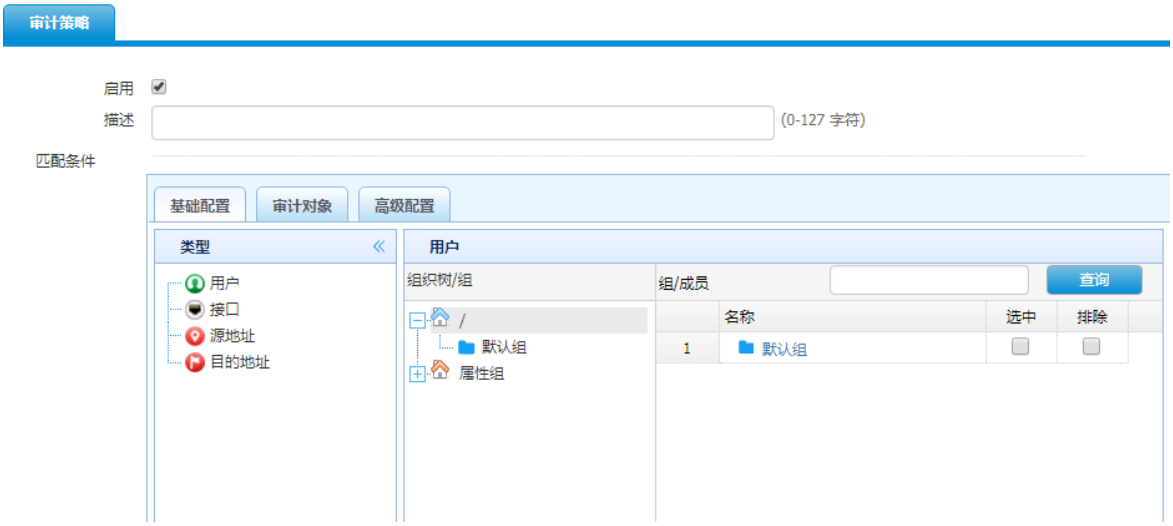


图1-10 审计策略详细配置页面 2-审计对象

图1-11 审计策略详细配置 3-高级配置

审计策略详细配置含义如表 1-8 所示。

表1-8 审计策略详细配置

标题项	说明
启用	新建策略默认勾选该项，表示策略启用；不勾选表示禁用状态。
描述	审计策略描述。
用户	匹配审计策略的用户对象。
接口	匹配审计策略的源目的接口/域。
源地址	匹配审计策略的源地址。
目的地址	匹配审计策略的目的地址。
HTTP	HTTP类审计对象，可以对HTTP类行为进行审计，主要包括网页访问、网络社区、网页搜索、HTTP文件上传下载、web网盘文件上传下载审计。
邮件	邮件类审计对象，可以对邮件类行为进行审计，主要包括SMTP、POP3、IMAP、Webmail收发邮件及附件审计。
即时通讯	即时通讯类审计对象，主要包括常用通讯软件QQ、微信、飞信等登录账号审计，以及收发消息行为审计，还有其它类通讯软件登录行为审计。
基础协议	基础协议类审计对象，主要包括FTP登录上传下载文件审计。
娱乐股票	娱乐股票类审计对象，主要包括娱乐股票类应用登录账号以及评论类审计。
网络应用	网络应用类审计对象，主要包括出上面具体应用行为外的其它一些应用行为进行审计。
时间	匹配审计策略的时间对象。
日志级别	审计策略日志记录级别，默认是信息级别，可以根据需求配置日志级别。
终端	匹配审计策略终端类型，默认是any所有终端类型，可以根据需求配置终端类型进行审计。

1.7 配置SSL证书推送

1.7.1 启用 SSL 证书推送

在导航栏中选择“策略配置 > SSL 解密策略 > SSL 证书推送”，进入证书推送页面，勾选启用按钮，配置 SSL 证书推送地址范围，进入如下图所示界面，在该界面，可以配置要进行证书推送的 IP 地址范文，各个配置项的含义如下表所示。

图1-12 新建端口镜像规则配置界面

表1-9 SSL 证书推送配置项含义

参数	说明
启用	是否启用SSL证书推送。
地址范围	SSL证书推送的IP地址范围。
排除地址	排除地址不进行SSL证书推送。

1.7.2 修改 SSL 证书推送

通过菜单“策略配置>SSL 解密策略>SSL 证书推送”，进入如下图所示的界面，在该界面上，可以修改证书推送地址，各个配置项的含义如下表所示。

图1-13 修改 SSL 证书推送

1.7.3 禁用 SSL 证书推送

在导航栏中选择“策略配置 > SSL 解密策略 > SSL 证书推送”，进入证书推送页面，不勾选启用按钮，如下图所示。禁用后系统将不进行 CA 证书的安装检测，对内网所有用户不进行 CA 证书的安装推送。

图1-14 禁用 SSL 证书推送

1.7.4 使用限制

- 当设备 DNS 设置成全局模式时，用户电脑的 DNS 需要指向设备的入接口，以保证 DNS 过设备。
- 证书推送检查基于 IP，无法支持多终端共享上网的情况，第一次检测后，一个小时内不再检测。
- 安卓手机、IOS 手机和 linux 系统的 PC 不支持证书推送。

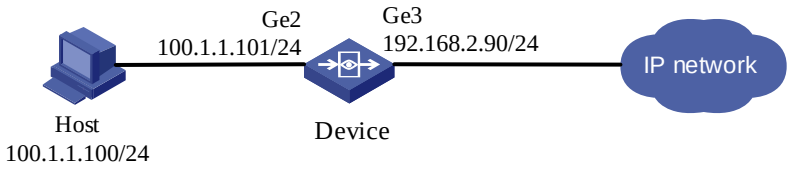
1.8 配置举例

1.8.1 解密策略配置案例

1. 组网需求

在 ge3 口上开启解密策略，记录审计日志。

图1-15 解密策略配置举例组网图



2. 配置步骤

(1) 配置 HTTPS 对象

在导航栏中选择“策略配置>对象管理>URL 对象>HTTPS 对象”，单击<新建>按钮，进入 HTTPS 对象配置界面，如图 1-16 所示。

图1-16 HTTPS 对象配置界面

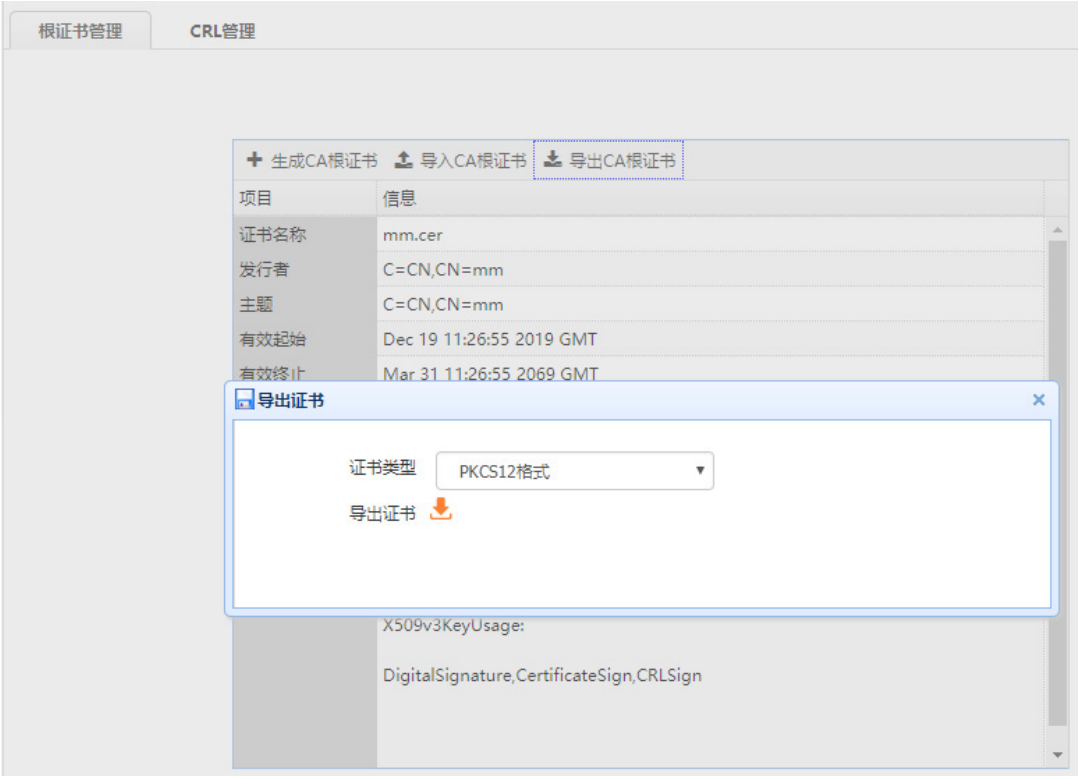
(2) 生成 CA 证书

如图 1-17 所示，进入“策略配置>对象管理>CA 服务器>根 CA 配置管理”，点击<生成 CA 根证书>。

图1-17 生成 CA 根证书

如图 1-18 所示，在生成 CA 证书以后，导出证书。.

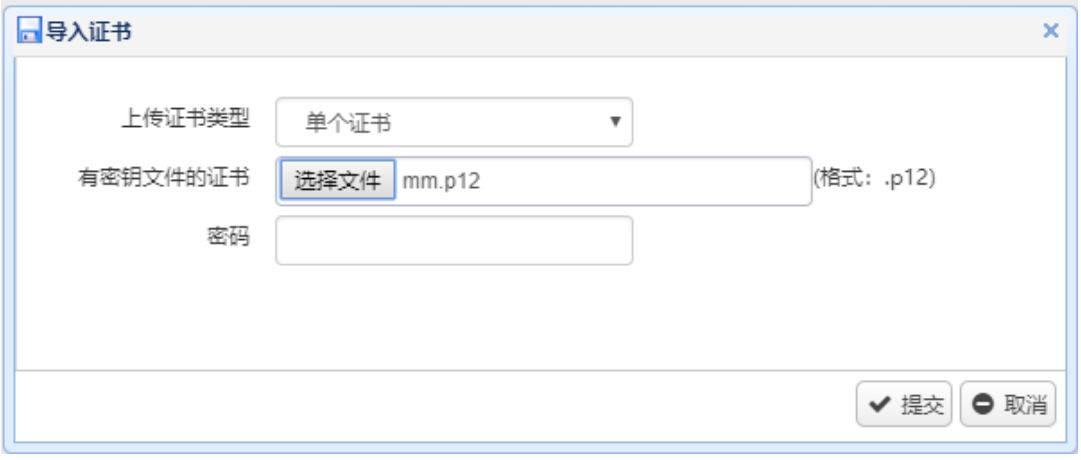
图1-18 导出 CA 证书



(3) 导入本地证书

在导航栏中选择“策略配置>对象管理>本地证书>证书>本地证书”，单击<导入>按钮，进入导入证书配置界面，如图 1-19 所示。

图1-19 导入证书界面



(4) 启用审计策略。

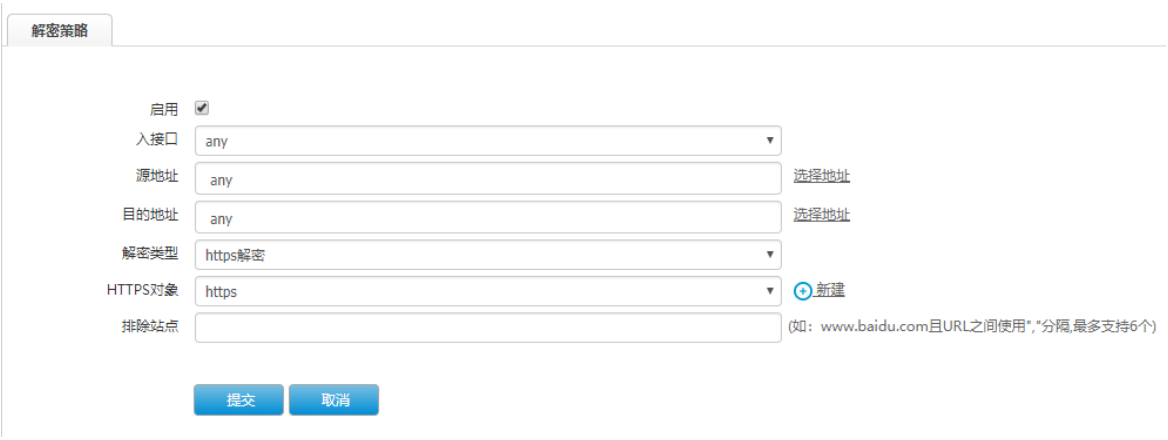
在导航栏中选择“策略配置 > 审计策略”，单击<新建>按钮，进入审计策略配置界面，选择所有审计对象，如图 1-20 所示。

图1-20 审计策略配置界面

(5) 配置解密策略

在导航栏中选择“策略配置>SSL 解密策略”，单击<新建>按钮，进入解密策略配置界面，如图 1-21 所示。

图1-21 解密策略配置界面



(6) 引用证书

在解密策略显示界面引用生成的证书“https.cer”，如图 1-22 所示。

图1-22 解密策略配置界面

3. 验证配置

进入“数据中心>日志中心>审计日志”，查看搜索引擎日志，如图 1-23 所示。

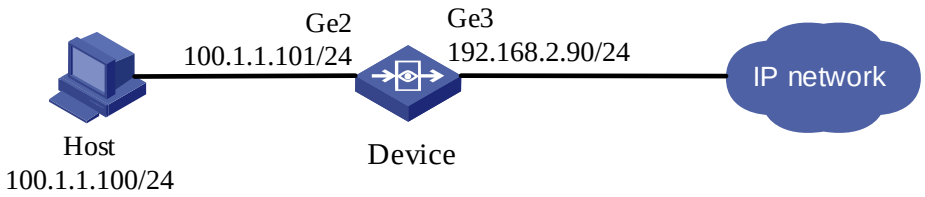
图1-23 搜索引擎日志界面

1.8.2 SSL 证书推送典型配置举例

1. 组网需求

针对内网地址为“100.1.1.100”的用户开启 SSL 证书推送，组网如下图所示。

图1-24 组网图



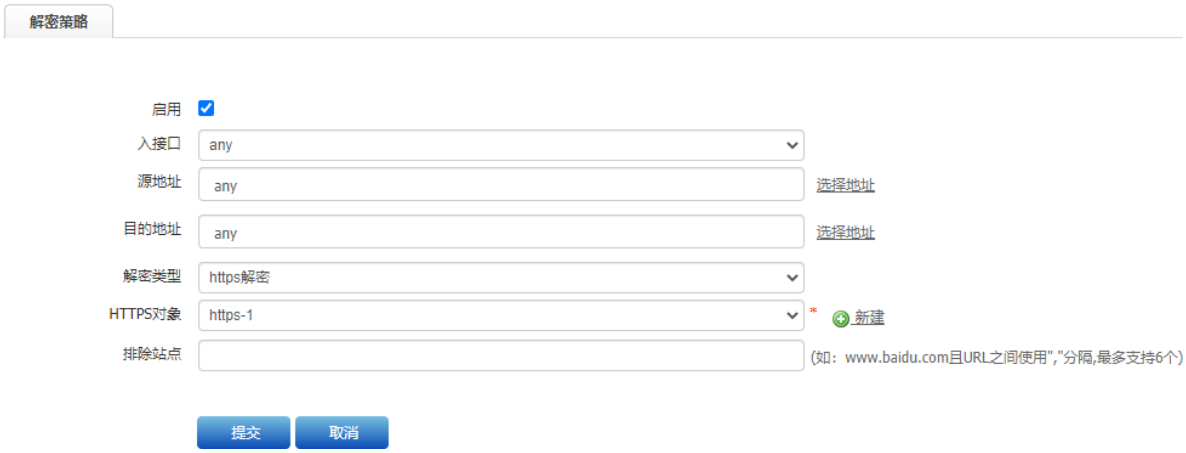
2. 配置注意事项

如果是网桥模式组网，配置步骤是一致的，需要注意的是网桥接口下一定要配置 IP 地址，并且要保证桥接口 IP 能访问外网。

3. 配置步骤

(1) 选择“策略配置 > SSL 解密策略”，单击“新建”按钮，配置解密策略，在证书列表中选择已配置的 HTTPS 对象，如下图所示。

图1-25 解密策略配置



(2) 在导航栏中选择“策略配置 > SSL 解密策略 > SSL 证书推送”，进入证书推送页面，勾选启用按钮，配置 SSL 证书推送地址范围，如下图所示。

图1-26 SSL 证书推送页面

4. 验证配置

(1) 配置完成后，使用地址为“100.1.1.100 的测试 PC 访问 http 地址，进入 302 重定向页面，如下图所示。

图1-27 验证结果

(2) 单击重定向页面的“下载证书”按钮，将证书文件下载到本地，如下图所示

图1-28 下载证书

(3) 安装证书。可单击重定向页面的“安装指导”下载安装说明，参考安装指导进行根证书的安装。

(4) 证书导入成功后，测试 PC 访问 HTTPS 网页，可以产生相应的审计日志。选择“数据中心 > 日志中心 > 审计日志 > 搜索引擎日志”界面，查看搜索引擎日志，如下图所示。

图1-29 搜索引擎日志界面

目 录

1 广告推送策略 ····· 1-1
1.1 概述 ····· 1-1
1.2 配置广告对象 ····· 1-1
1.3 配置广告策略 ····· 1-2
1.4 配置举例 ····· 1-3
1.4.1 广告设置配置举例 ····· 1-3

1 广告推送策略

1.1 概述

广告推送是一种在用户使用浏览器上网的同时，网络设备强制浏览器打开特定的广告窗口的方法。按某种规则给用户浏览器弹出一个广告页面，以达到广告推广或者提示用户的目的。

1.2 配置广告对象

通过菜单“策略配置>广告推送策略>广告对象”，点击新建进入如图 1-1 所示界面，在该界面上，可以配置广告对象信息，这些信息的详细说明如表 1-1 所示。

图1-1 广告对象配置界面

表1-1 广告对象配置说明

参数	说明
广告名称	广告对象名称。
广告描述	广告进行描述，不会在弹出广告页面显示。
广告类型	可选本地自定义广告和第三方广告，默认显示本地自定义广告。
设备管理IP	广告对象里的管理IP必须保证可以和下联终端互通，否则开启广告后网页无法打开。
位置	广告图片展示的位置，默认右下角，可以选择右下角、右上角、左下角、左上角。

参数	说明
广告图片	上传图片后在本地广告里面引用的弹出图片，最多可以展示4张，每张图片默认展示3秒，加上1秒缓冲。例如4张图片4*3+1=13秒。图片规格：推荐340px*260px
图片描述	广告图片可以添加描述信息范围（0-31字符）。
图片URL	当广告图片展示时点击图片的链接URL。
广告对象选择文件按钮	上传本地广告图片使用。
广告对象开始上传按钮	广告图片配置完成后上传使用。
广告对象已存在按钮	上传图片后可以查看上传图片。
本地广告取消重选按钮	更改图片后不需要修改的情况下点击取消按钮返回上一次上传的图片。
第三方广告URL	第三方广告需要配合第三方广告服务器使用，除了serverip需要填写外其它参数为动态参数，如果用户URL里输入了参数，且参数后边是<>，说明该参数用户需要，且底层根据实际数据流的信息给参数赋值，但是如果URL里输入了参数，参数等号后边是直接的值，是需要用户直接配置下来的，底层根据用户的配置信息来组织js。
提交按钮	所有参数配置完成后，点击提交生效。
取消按钮	所有参数配置完成后，点击取消按钮后，不会生效。

1.3 配置广告策略

通过菜单“策略配置>广告推送策略>广告策略”，点击新建进入如图 1-2 所示界面，在该界面上，可以配置广告推送策略，配置信息的详细说明如表 1-2 所示。

图1-2 广告策略配置界面

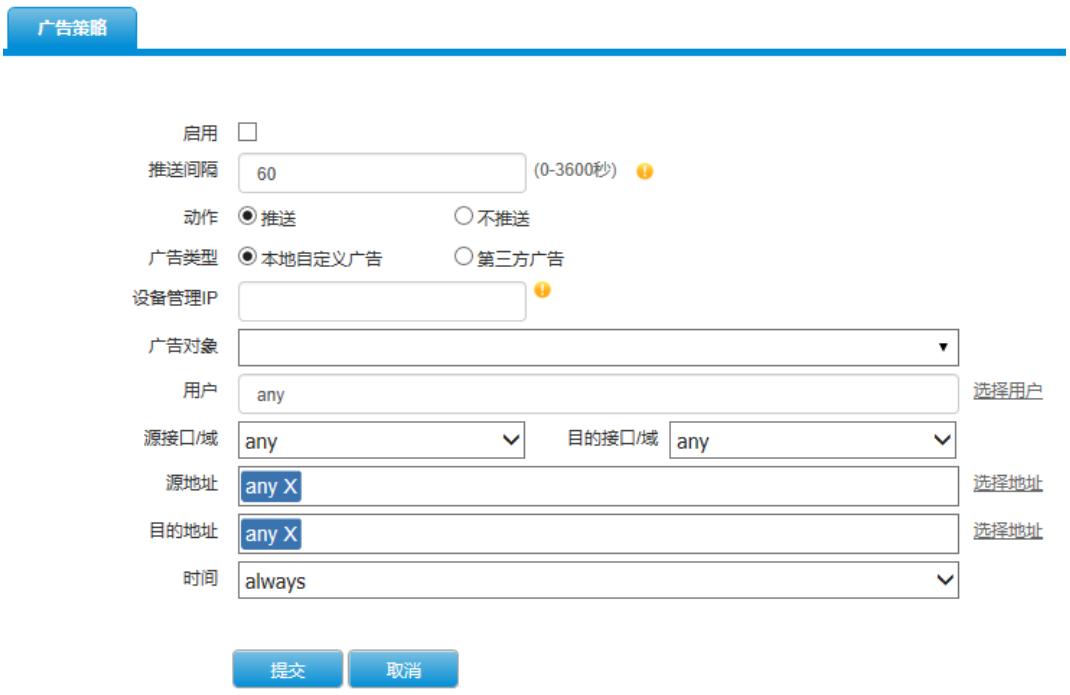


表1-2 广告策略配置说明

参数	说明
启用	广告策略启用开关。
推送间隔	范围0-3600秒，针对单个用户弹出广告间隔设置，同一用户在一定间隔内不会重复弹送广告，如果配置为0会一直推送广告。
动作	推送和不推送。默认推送，当广告策略启用且选择了不推送后，该策略不生效，继续匹配下一跳广告策略
广告类型	可选本地自定义广告和第三方广告，默认显示本地自定义广告。当选择好广告类型后，广告对象不能交叉引用
设备管理IP	设备管理IP为选配项可为空，若配置优先使用配置IP，否则使用报文入接口IP，两者均为获取到则不弹广告；配置管理IP务必保证用户可达，否则无法加载原始页面
广告对象	调用配置好的广告对象。
IPV4策略	用户：匹配策略的用户或用户组对象。 源接口/域：策略指定源接口。 目的接口/域：策略指定目的接口。 源地址：匹配策略源地址。 目的地址：匹配策略目的地址。 时间：匹配策略的时间对象。

1.4 配置举例

1.4.1 广告设置配置举例

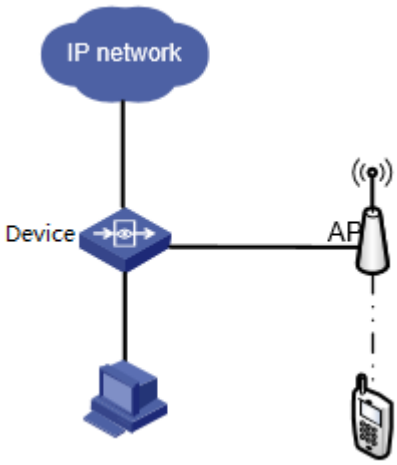
1. 组网需求

在公司出口网关开启广告设置，推送公司的一些活动或者提示用户一些信息如图 1-3 所示。

- 将来自 192.168.1.0/24 网线上网的客户弹出广告推广
- 将来自 192.168.2.0/24 无线 AP 上网的手机客户弹出广告推广

2. 组网图

图1-3 广告设置配置案例组网图

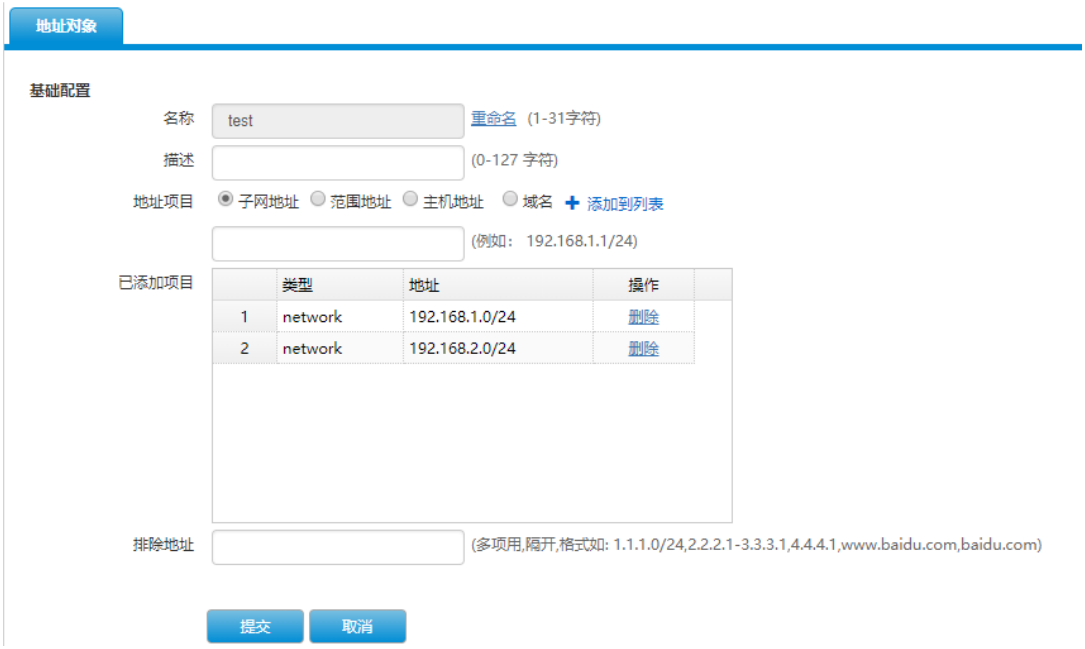


3. 配置步骤

(1) 按照组网图组网

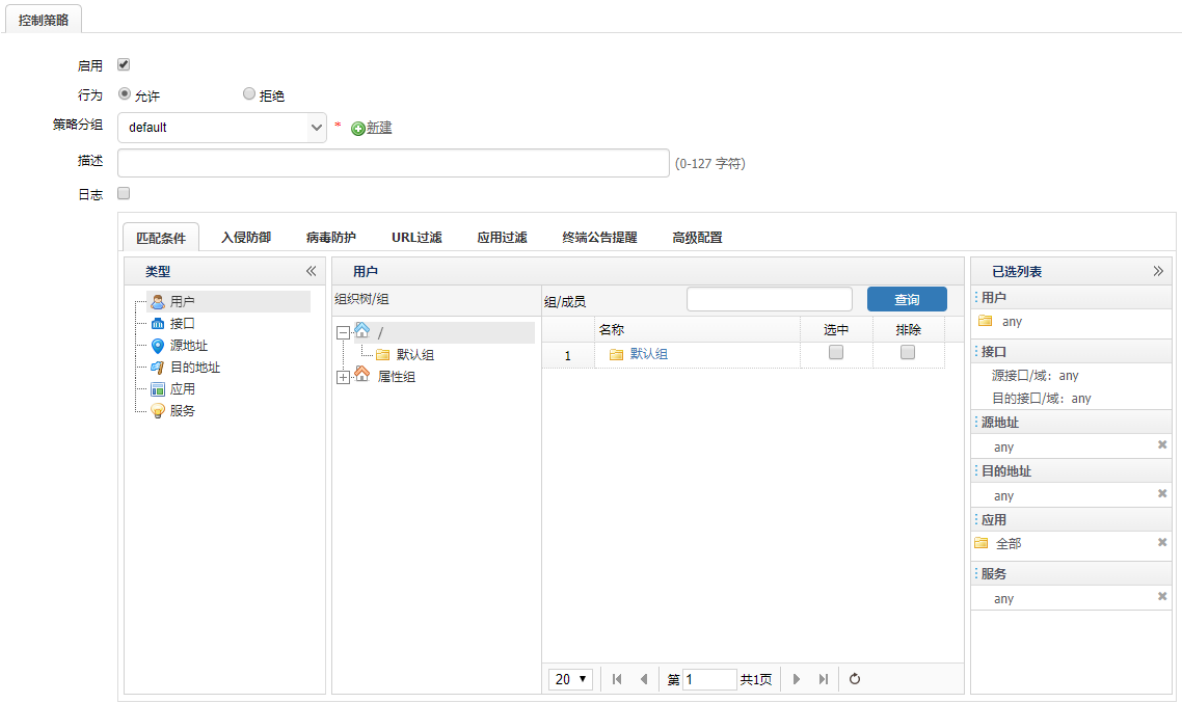
(2) 配置地址对象，如图 1-3 所示

图1-4 配置地址对象



(3) 通过菜单“策略配置 > 控制策略”，点击<新建>，进入如图 1-55 所示的页面。行为选择“允许”，其它为默认，配置一条全通策略。

图1-5 控制策略配置



(4) 通过菜单“策略配置>广告推送策略>广告对象”，单击“新建”按钮，如图 1-66 所示

图1-6 广告对象

(5) 通过菜单“策略配置>广告推送策略>广告策略”，单击“新建”按钮，如图 1-77 所示。根据不同的用户或者用户组配置不同的广告对象，源地址配置地址对象 test。

图1-7 广告策略

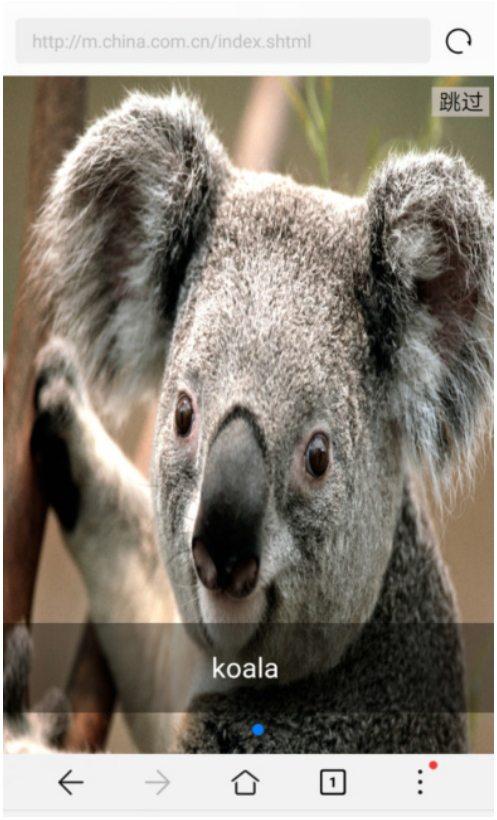
4. 验证配置

如图 1-8 所示，使用 PC 访问外网 HTTP 网站会弹出广告图片。

图1-8 PC 访问外网 HTTP 网站显示页面

如图 1-9 所示，使用手机访问外网 HTTP 网站会弹出广告图片。

图1-9 手机访问外网 HTTP 网站显示页面



目 录

1 会话限制配置 ····· 1-1
1.1 会话限制简介 ····· 1-1
1.2 会话限制新建 ····· 1-1
1.3 会话限制修改 ····· 1-2
1.4 限制阻断 ····· 1-2
1.5 配置举例 ····· 1-3
1.5.1 会话限制配置举例 ····· 1-3

1 会话限制配置

1.1 会话限制简介

通过会话限制（session-limit）的策略配置，可以将指定的用户 IP 连接数控制在一定范围内，并且可以基于 IP 统计现有的连接数。该功能可基于 IP 对 session 数的统计，地址对象 IP 发起连接数控制（支持全网段地址），并有阈值报警功能，控制是对指定的地址对象中的每一个 IP 而言。

1.2 会话限制新建

点击导航栏的“策略配置 > 会话控制管理”，进入会话限制的显示页面，如图 1-1 所示。在每 IP 会话限制页面中，点击<新建>按钮，会切换到新建的页面，如图 1-2 所示。

图1-1 会话限制显示界面

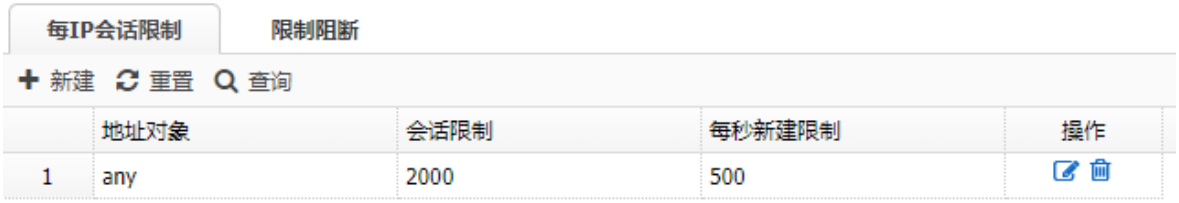


图1-2 会话限制配置页面

表1-1 会话限制详细信息描述表

配置项	说明
地址对象	可引用已配置成功的地址对象，缺省情况下包含“any”和“private”。
会话限制	当前地址对象中每个IP地址能存在的最大会话数。
每秒新建限制	当前地址对象中每个IP地址每秒能创建的最大会话数。

1.3 会话限制修改

如图 1-3 所示，点击导航栏的“策略配置 > 会话控制管理 > 每 IP 会话限制”，进入会话限制的显示页面。在每 IP 会话限制页面中，点击对应地址对象后的<编辑>按钮，会切换到编辑的页面，可以对所选地址对象的会话限制数、每秒新建限制数进行编辑。

图1-3 会话限制编辑界面

1.4 限制阻断

如图 1-4 所示，点击导航栏的“策略配置 > 会话控制管理”，再点击限制阻断标签页，显示设备上被阻断的 IP 的信息。

图1-4 限制阻断界面

表1-2 限制阻断详细信息描述表

配置项	说明
查询	要查找的指定的IP信息

说明

只有配置了会话限制，才会进行限制阻断的统计。

1.5 配置举例

1.5.1 会话限制配置举例

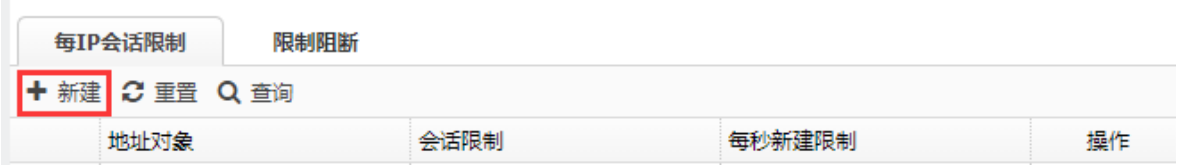
1. 用户需求

对用户 any 进行会话限制，会话数和每秒新建数都限制为 10，配置完成后查看其限制结果。

2. 配置步骤

(1) 如图 1-5 示，通过菜单“策略配置 > 会话控制管理 > 每 IP 会话限制”打开会话限制页面。

图1-5 会话限制显示



(2) 如图 1-6 所示，点击<新建>按钮，在弹出的页面进行配置并提交。

图1-6 会话限制新建页面

3. 验证配置

(1) 如图 1-7 所示，回到显示页面，可以看到我们配置的规则。

图1-7 会话限制显示

(2) 如图 1-8 所示，点击限制阻断，可以看到会话限制的结果。以 IP198.168.200.36 为例，我们可以看到它当前的连接数被限制为 10，再看限制阻断统计那一项，我们可以看到，有 1737 个会话连接被阻断了。

图1-8 限制阻断页面

	IP地址	连接数	会话限制	每秒新建	每秒新建限制	限制阻断统计	地址对象
1	192.168.200.36	8	10	0	10	1737	any
2	192.168.8.99	10	10	0	10	32	any
3	192.168.200.37	1	10	0	10	0	any
4	192.168.200.173	1	10	0	10	0	any
5	192.168.200.182	1	10	0	10	0	any

目 录

1 共享上网监控 ····· 1-1
1.1 简介 ····· 1-1
1.2 共享接入配置 ····· 1-1
1.3 共享接入监控 ····· 1-2
1.4 共享接入公告 ····· 1-3
1.5 共享上网监控配置举例 ····· 1-4
1.5.1 组网需求 ····· 1-4
1.5.2 组网图 ····· 1-5
1.5.3 配置步骤 ····· 1-5
1.5.4 验证配置 ····· 1-6

1 共享上网监控

1.1 简介

在很多用户场景下，从运营商分配的一个帐号被多个用户共享使用，导致去运营商开户的用户数量骤减；同时在多人使用同一账号上网后，无法精确追踪上网记录到个人，存在安全隐患；因此运营商需要共享上网识别与控制来提升自己的开户量，为其创造价值。

1.2 共享接入配置

通过菜单“策略配置>共享接入管理>共享接入配置”，进入如图 1-1 所示页面。在该页面上可以配置共享接入检测的相关功能。

图1-1 共享接入配置页面

共享接入配置各项参数含义如表 1-1 所示。

表1-1 共享接入配置项含义表

标题项	说明
用户共享检测	勾选复选框表示开启共享上网监测。
检测方式	默认支持5种检测方式，分别为：时间戳、UA识别、应用特征、Flash Cookie、微信长连接。
发送日志	启用发送日志后，当用户共享被阻断或限速时会发送共享接入日志。

标题项	说明
阈值设置	终端阈值：单个IP下允许接入终端的临界值，当达到该值时根据惩罚方式进行处理，小于该值时可以正常接入。终端阈值的范围为2-20个； 允许例外情况：可以配置单个IP下电脑和移动终端的数量。
惩罚方式	• 无：表示不惩罚，只做检测； • 阻断：表示检测到共享接入用户达到阈值之后，进行阻断惩罚操作；阻断提示可在公告页面进行自定义配置； • 限速：表示检测到共享接入用户达到阈值之后，进行限速惩罚操作； 冻结/限速时长：选择阻断或者限速惩罚方式时，显示该页面配置；终端被冻结或限速的时间，范围为5-720分钟； 添加到流控通道：选择限速惩罚方式时，需要选择对应的限速流控通道配置。
启用信任用户	勾选该项，已配置的用户或IP地址检测到共享接入之后将不进行惩罚。 白名单分为用户、信任IP（范围地址和主机地址）： • 用户：可选择用户组及成员； • 范围地址：如 192.168.1.1-192.168.1.10； • 主机地址：如 192.168.1.1。

1.3 共享接入监控

通过菜单“策略配置>共享接入管理>共享接入监控”，进入如图 1-2 所示页面。在该页面上可以查看设备监控共享上网情况。

图1-2 共享接入监控页面

共享接入监控各项参数含义如表 1-2 所示。

表1-2 共享接入监控含义表

标题项	说明
用户名	显示设备存储ip地址对应的用户名。
所属组	显示设备存储用户加入的用户组。
IP	显示终端IP地址。
MAC	显示终端MAC地址。
终端数量	共享设备下面的终端数。
终端类型	终端接入类型。
状态	显示共享接入用户的状态类型；正常、阻断、限速。
发现时间	显示发现共享接入用户的时间。

标题项	说明
操作	可以选择是否解除惩罚共享接入的用户。

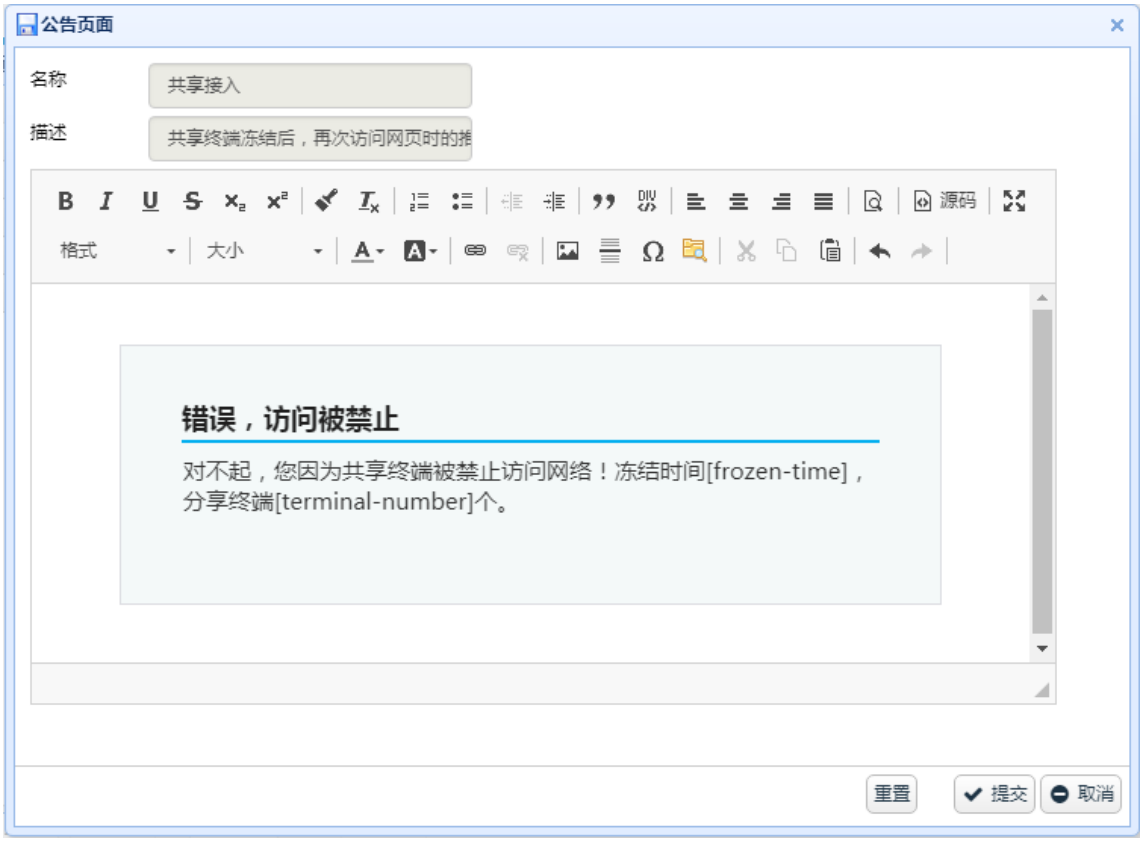
1.4 共享接入公告

通过菜单“策略配置> 对象管理 > 公告页面 > 其它页面”，进入如图 1-3 所示页面。在该页面上可以查看设备共享接入公告阻断提示配置，也可以自定义修改配置。

图1-3 共享接入公告页面

点击蓝色字体<共享接入>，进入共享接入公告页面配置进行阻断提示配置。如图 1-4 所示。

图1-4 共享接入阻断提示配置



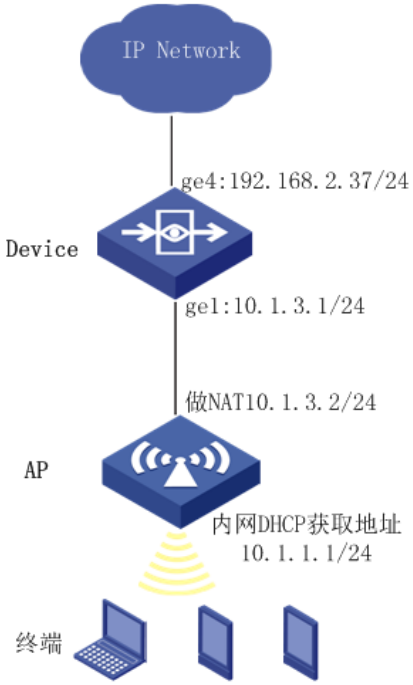
1.5 共享上网监控配置举例

1.5.1 组网需求

- 终端通过 wifi 上网，多个终端共享一个 wifi 通过设备访问外网。
- 设备和终端网络可达。

1.5.2 组网图

图1-5 共享上网监控组网图



1.5.3 配置步骤

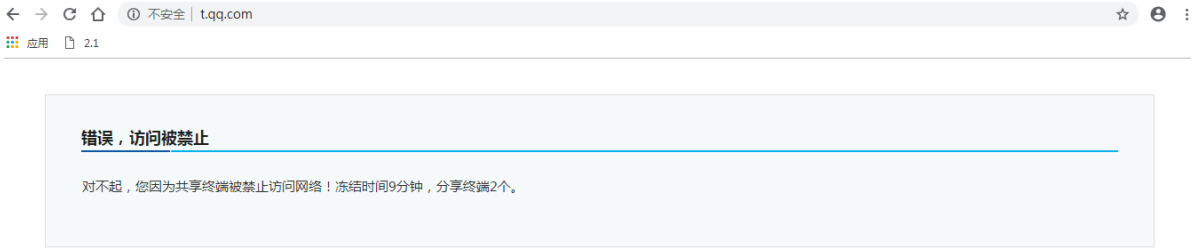
(1) 共享接入参数配置。如图 1-6 所示。

图1-6 共享接入参数配置

1.5.4 验证配置

(1) 配置完成后，使用多个终端连接 wifi 通过设备访问外网，当检测到访问网络共享用户达到 2 个时，终端访问外网自动被阻断。如图 1-7 所示。

图1-7 共享接入终端阻断提示

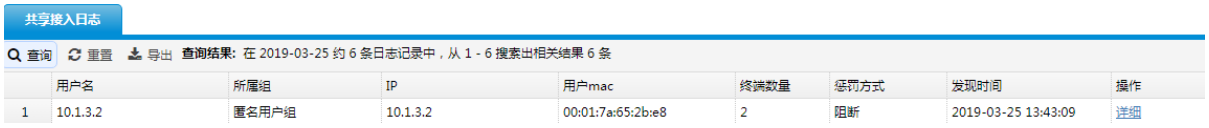


(2) 在共享接入监控页面，可以查看已被监控到的共享接入用户信息，如图 1-8 所示。

图1-8 共享接入监控

(3) 共享日志处能查看到具体的共享接入阻断日志，如图 1-9 所示。

图1-9 共享接入阻断日志



说明

- 终端用户达到阈值被阻断时，需要配置解密类型为 HTTPS 解密的 SSL 解密策略，且 HTTPS 对象需包含访问 HTTPS 页面的域名，用户访问 HTTPS 页面才可以弹出阻断提示信息。
- 惩罚方式配置限速的，优先需要在流控策略上配置惩罚通道，共享用户达到阈值被限速时，用户不会弹出相关提示信息，只是访问外网被限速。
- 启用信任用户，支持用户、IP 地址范围、IP 主机地址三种，配置了信任的用户达到阈值之后将不会惩罚，只检测。

目 录

1 移动终端管理 ····· 1-1
1.1 移动终端管理简介 ····· 1-1
1.2 移动终端管理页面 ····· 1-1
1.3 终端接入配置 ····· 1-2
1.4 终端发现趋势 ····· 1-3
1.5 典型配置举例 ····· 1-4
1.5.1 组网需求 ····· 1-4
1.5.2 配置思路 ····· 1-4
1.5.3 配置步骤 ····· 1-4
1.5.4 验证配置 ····· 1-9

1 移动终端管理

1.1 移动终端管理简介

随着智能手机、Pad 等轻薄便携的移动智能终端与人们的生活、工作和学习结合得越来越紧密，随之而来的内网管控的问题。更多的移动终端接入内网需要进行管控，移动终端管理可针对移动终端进行管控。

1.2 移动终端管理页面

通过菜单“策略配置 > 移动终端管理”，进入如图 1-1 所示页面。在该页面上可以查看移动终端管理识别并进行操作。各个配置项含义如表 1-1 所示。

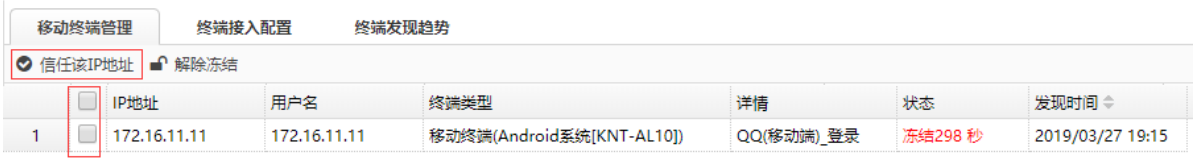
图1-1 移动终端管理页面

表1-1 移动终端管理页面各项含义表

标题项	说明
IP地址	设备记录的移动终端IP地址。
用户名	设备记录的移动终端用户名。
终端类型	设备记录的移动终端型号。
详情	移动终端识别详情。
状态	移动终端状态： ● 正常：只检测，不进行冻结； ● 冻结XX秒：移动终端被冻结。
发现时间	移动终端检测发现时间。

选中移动终端后，点击<信任该 IP 地址>，可将此 IP 地址添加到信任 IP 中，如图 1-2 所示。

图1-2 信任该 IP 地址



选中移动终端后，点击<解除冻结>，可将已冻结用户暂时解除冻结状态，如图 1-3 所示

图1-3 解除冻结

1.3 终端接入配置

通过菜单“策略配置 > 移动终端管理”，点击<终端接入配置>页签，进入如图 1-4 所示页面。在该页面上可以配置终端接入配置。各个配置项含义如表 1-2 所示。

图1-4 终端接入配置页面

表1-2 终端接入配置页面各项含义表

标题项	说明
启用移动终端管理	启用/禁用移动终端管理功能。

标题项	说明
配置告警邮件	配置告警邮件链接，可以点击跳转到配置页面。
冻结上网	启用/禁用冻结上网功能。启用后会限制移动终端上网。
冻结时长	配置冻结时间。
启用信任用户	启用/禁用信任用户功能，启动后可选择信任用户。
信任IP	支持子网地址、范围地址、主机地址三种方式添加，点击<添加到列表>，可以添加信任IP地址。

1.4 终端发现趋势

通过菜单“策略配置 > 移动终端管理”，点击<终端发现趋势>页签，进入如图 1-5 所示页面。在该页面上可以查看终端发现趋势。各个配置项含义如表 1-3 所示。

图1-5 终端发现趋势页面

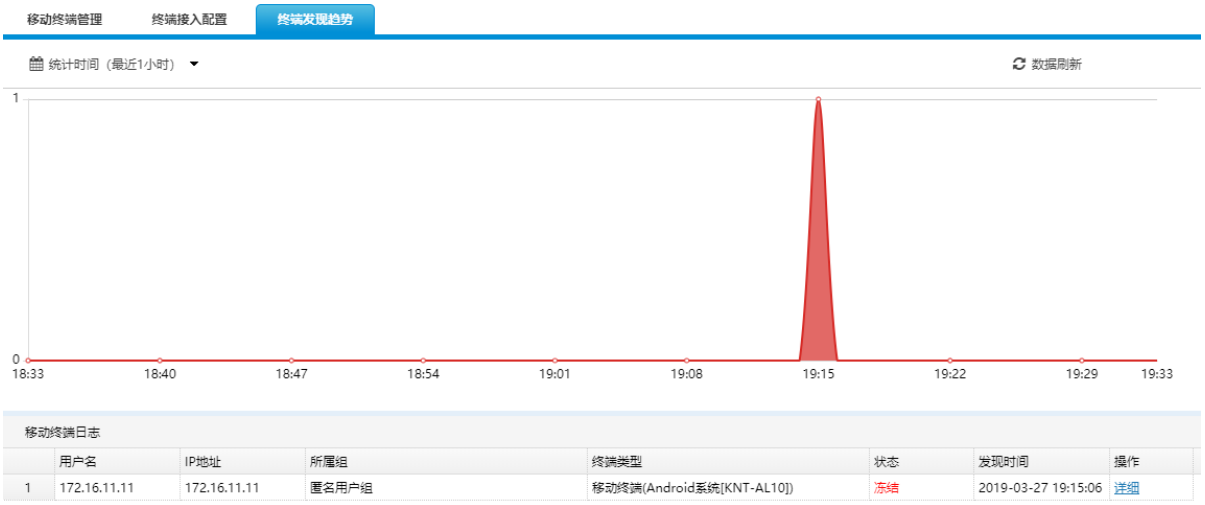


表1-3 终端发现趋势页面各项含义表

标题项	说明
用户名	设备记录移动终端的用户名。
IP地址	设备记录移动终端的IP地址。
所属组	设备记录移动终端所属用户组。
终端类型	设备记录的移动终端型号。
状态	移动终端状态： ● 正常 ● 冻结
发现时间	移动终端发现时间。
操作	点击<详细>，展示详细信息。

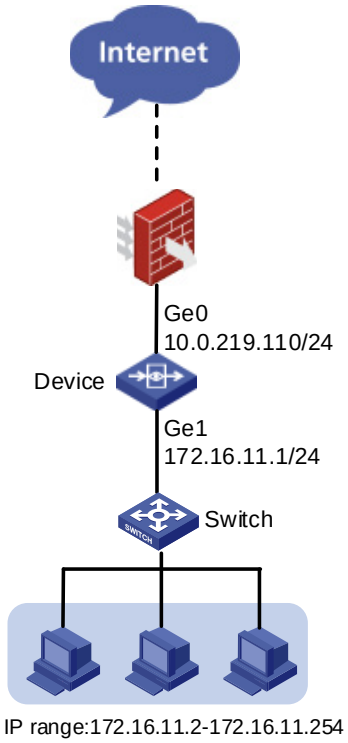
1.5 典型配置举例

1.5.1 组网需求

如图 1-6 所示，某公司为了提高工作效率，实行移动终端管理上网控制。要求除固定地址可以接入移动终端，其余地址不允许接入移动终端设备。使用设备的 ge0 和 ge1 接口透明模式部署在网络中，在设备上配置移动终端管理功能。具体要求如下：

- 公司内网地址段：172.16.11.1/24。
- 可以接入移动终端地址：172.16.11.17。

图1-6 移动终端管理配置组网图



1.5.2 配置思路

- 配置地址对象。
- 配置用户识别范围。
- 配置移动终端管理策略。

1.5.3 配置步骤

(1) 配置地址对象

如图 1-7 所示，进入“策略配置>对象管理> 地址对象”，点击<新建>，配置“内网地址”为 172.16.11.1/24，点击<提交>。

图1-7 配置地址对象

(2) 配置用户识别范围

如图 1-8 所示，进入“用户管理>认证管理>高级选项”，进入全局配置页面，点击识别范围选择框，选择<内网地址>地址对象，点击<提交>。

图1-8 配置用户识别范围

(3) 配置移动终端管理策略

如图 1-9 所示，进入“策略配置>移动终端管理”，点击<终端接入配置>页签，进入终端接入配置页面，勾选 <启用移动终端管理>按钮，点击<提交>。

图1-9 终端接入配置页面

(4) 配置移动终端冻结

如图 1-10 所示，进入“策略配置>移动终端管理”，点击<终端接入配置>页签，进入终端接入配置页面，勾选 <冻结上网>按钮，可以修改冻结时长，在信任 IP 中添加 172.16.11.17 地址，点击<提交>。

图1-10 配置移动终端冻结

(5) 配置终端告警

如图 1-11 所示，进入“策略配置>移动终端管理”，点击<终端接入配置>页签，进入终端接入配置页面，点击<配置告警邮件>链接，在弹出页面，开启移动终端告警功能，点击<提交>。

图1-11 配置终端告警

(6) 配置邮件告警

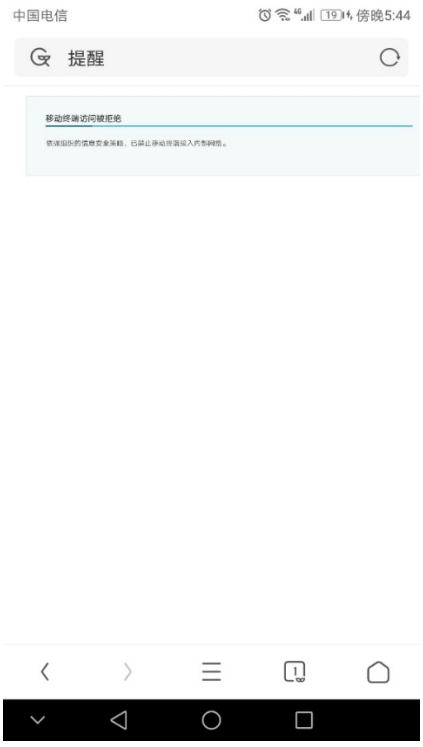
如图 1-12 所示，在终端接入配置页面，点击<配置告警邮件>链接，在弹出页面，配置邮件功能，点击<提交>。

图1-12 配置邮件告警

1.5.4 验证配置

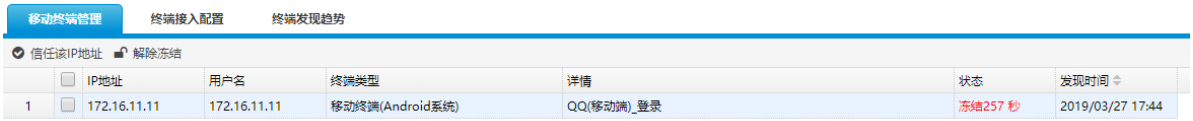
如图 1-13 所示，内网用户使用移动终端访问网站时，会被阻断且有阻断提示。

图1-13 移动终端冻结验证



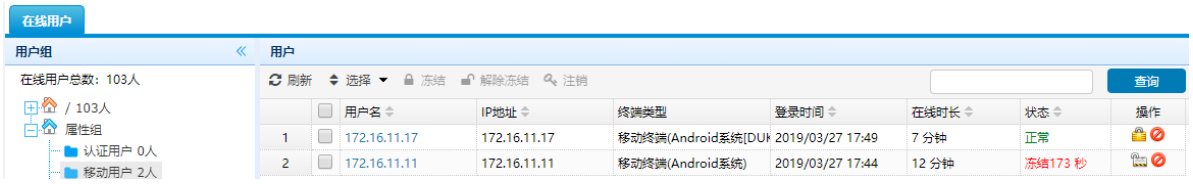
如图 1-14 所示，进入“策略配置>移动终端管理”，进入移动终端管理页面，可以查看到移动终端阻断信息。

图1-14 移动终端阻断信息



如图 1-15 所示，进入“数据中心>系统监控>在线用户”，进入在线用户页面，可以查看到 172.16.11.17（信任 IP）地址的移动终端可以正常上网。

图1-15 信任 IP 验证



如图 1-16 所示，开启了邮件告警功能，可以在邮件中收到设备发送的告警邮件。

图1-16 邮件告警验证

目 录

1 全局白名单 ····· 1-1
1.1 全局白名单简介 ····· 1-1
1.2 配置全局白名单 ····· 1-1
1.3 全局白名单典型配置举例 ····· 1-3
1.3.1 组网需求 ····· 1-3
1.3.2 组网图 ····· 1-3
1.3.3 配置步骤 ····· 1-3
1.3.4 验证配置 ····· 1-5

1 全局白名单

1.1 全局白名单简介

当前的网络环境中，出于信息安全的考虑对用户上网的数据进行控制和审计的限制；但是存在一些特权的用户（高层领导、特权管理员），他们不希望自己上网的数据被限制或者被审计；全局白名单可以针对特殊用户排除这些繁琐的策略审计，实现数据全放通。

本功能具有如下功能点：

- 支持对源 IP 地址配置（包括主机地址、网段地址、地址范围）配置白名单；
- 支持对源 MAC 地址配置白名单；
- 该功能支持 IPv4/IPv6 的使用场景。

1.2 配置全局白名单

通过菜单“策略配置 > 全局白名单”，进入如图 1-1 所示页面。在该页面上可以查看已配置的全局白名单信息，各个显示项含义如表 1-1 所示。

图1-1 全局白名单页面

表1-1 全局白名单配置项含义表

标题项	说明
名称	全局白名单策略的名称，必填项。
地址	配置全局白名单的地址，可支持配置IP地址和MAC地址两种方式。
描述	全局白名单策略的描述，选填项。
状态	全局白名单策略的状态分启用和禁用两种状态。
操作	操作选项可以对全局白名单策略执行编辑修改描述、地址、状态操作，也可以删除单条全局白名单策略操作。

点击图 1-1 的<新建>按钮，可以进入全局白名单配置界面，如图 1-2 所示。各个配置项的含义如表 1-2 所示。

图1-2 全局白名单配置页面

表1-2 全局白名单配置项含义表

标题项	说明
启用	全局白名单策略是否启用，勾选表示启用，不勾选表示禁用。
名称	全局白名单策略的名称，必填项。
描述	全局白名单策略的描述，选填项。
地址	配置全局白名单的地址，可支持配置IP地址和MAC地址两种方式。

说明

- 全局白名单只对会话中的源 IP、源 MAC 进行匹配。
- 配置全局白名单的用户仅做会话识别，不做其它控制策略。

1.3 全局白名单典型配置举例

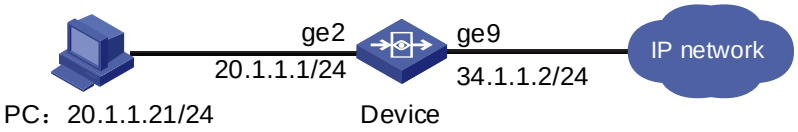
1.3.1 组网需求

测试终端通过设备访问外网资源，设备对测试终端所有用户（图中测试终端 PC 除外）访问外网资源进行审计并对终端访问外网要优先进行 WEB 认证，以及工作时间禁止使用即时通讯软件。

- 测试终端和设备网络可达。
- 设备上用户识别范围包含测试终端所在网段。

1.3.2 组网图

图1-3 全局白名单组网图



1.3.3 配置步骤

(1) 配置用户识别范围。如图 1-4 所示。

图1-4 配置用户识别范围

(2) 配置审计策略。如图 1-5 所示。

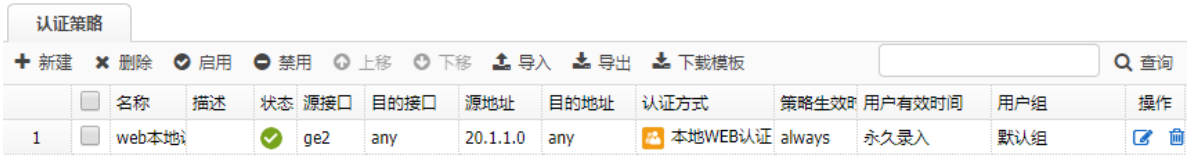
图1-5 审计策略配置页面

(3) 配置控制策略。如图 1-6 所示。

图1-6 控制策略配置

(4) 配置认证策略。如图 1-7 所示。

图1-7 认证策略配置



(5) 配置全局白名单，如图 1-8 所示。

图1-8 配置全局白名单

1.3.4 验证配置

配置完成后，在白名单用户测试 PC（20.1.1.21）上访问外网不需要经过认证即可上网，且上网访问的记录将不会进行审计，工作时间登录 qq 也是正常的。

在其它非白名单用户终端（20.1.1.10）上访问外网首先需要进行认证才能访问外网，且访问外网的相关记录设备上可以进行审计，工作时间登录 qq 被阻断。

(1) 非白名单用户访问外网需要优先进行认证，如图 1-9 所示。

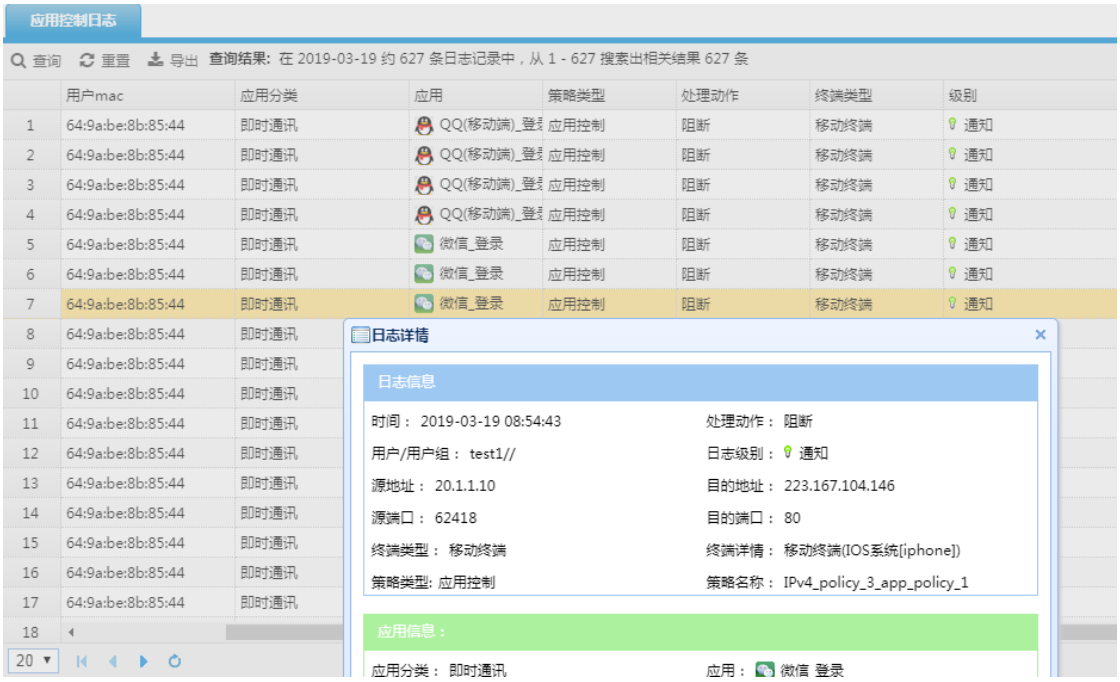
图1-9 非白名单用户访问外网优先进行认证

(2) 非白名单用户浏览网页审计记录正常，如图 1-10 所示。

图1-10 非白名单用户访问网页审计日志

(3) 非白名单用户即时通讯软件阻断正常，如图 1-11 所示。

图1-11 非白名单用户登录即时通讯软件被阻断



目 录

1 入侵防御 ····· 1-1
1.1 入侵防御概述 ····· 1-1
1.2 入侵防御规则模板配置 ····· 1-2
1.2.1 规则模板页面 ····· 1-2
1.2.2 新建规则模板 ····· 1-2
1.2.3 派生规则模板 ····· 1-3
1.2.4 查看规则列表 ····· 1-4
1.2.5 添加规则 ····· 1-5
1.2.6 修改规则配置 ····· 1-6
1.2.7 查询事件 ····· 1-7
1.3 入侵防御协议异常检测 ····· 1-8
1.3.1 协议异常检测简介 ····· 1-8
1.3.2 协议异常检查页面 ····· 1-8
1.3.3 HTTP 协议异常检查 ····· 1-9
1.3.4 DNS 协议异常检查 ····· 1-11
1.3.5 SMTP 协议异常检查 ····· 1-12
1.3.6 POP3 协议异常检查 ····· 1-13
1.3.7 FTP 协议异常检查 ····· 1-15
1.4 入侵防御自定义规则 ····· 1-16
1.4.1 入侵防御自定义规则简介 ····· 1-16
1.4.2 入侵防御规则库显示 ····· 1-16
1.4.3 入侵防御自定义规则配置 ····· 1-16
1.4.4 协议字段的配置 ····· 1-17
1.5 入侵防御防逃避 ····· 1-20
1.5.1 入侵防御防逃避简介 ····· 1-20
1.5.2 入侵防御防逃避 命令行 ····· 1-20
1.6 入侵防御策略 ····· 1-21
1.7 入侵日志聚合 ····· 1-22
1.8 入侵日志告警规则 ····· 1-23
1.9 入侵防御配置举例 ····· 1-24
1.9.1 组网需求 ····· 1-24
1.9.2 配置思路 ····· 1-24
1.9.3 配置注意事项 ····· 1-25

1.9.4 配置步骤 ·····1-25
1.9.5 验证配置 ·····1-27

1 入侵防御

1.1 入侵防御概述

随着互联网的飞速发展，网络环境也变得越来越复杂，恶意攻击、木马、蠕虫病毒等混合威胁不断增大，单一的防护措施已经无能为力，企业需要对网络进行多层、深层的防护来有效保证其网络安全，而入侵防御系统则是提供深层防护体系的保障。

入侵防御涉及以下概念：

- 规则模板：规则模板是一个或多个规则的集合，规则模板分为预定义规则模板、派生规则模板和自定义规则模板。

  预定义规则模板由系统自动创建，其中包含的规则以及每条规则的配置（阻断、抓包等）也都由系统预先设定，规则不允许增加或删除，每条规则的配置也不允许修改。预定义规则模板包括以下四个：

  - all：包含全部规则
  - web：包含 HTTP 相关规则
  - windows：包含 Windows 系统漏洞规则
  - unix：包含 Unix、Linux 系统漏洞规则

  预定义规则模板下每条规则的配置初始值如下：

  - 日志：根据规则严重程度确定，严重程度为“高”，日志默认为告警；严重程度为“中”，日志默认为警告；严重程度为“低”，日志默认为“通知”。
  - 阻断：默认阻断。
  - 隔离：默认不隔离。
  - 抓包：默认不抓包。

  派生规则模板由预定义规则模板派生而来，其中包含的规则与对应的预定义规则模板相同，也是不允许增加或删除，但是可以修改每条规则的配置。派生规则模板由用户根据需要手动派生创建，派生规则模板不可以再派生。

  自定义规则模板完全由用户自己定义创建，其中包含的规则以及配置都可以随意修改。

- 规则：规则除了包含有检测攻击的特征之外，还有规则严重程度、规则状态、日志、阻断、隔离、抓包，CVE、CNNVD、操作系统、发布年份、厂商，操作等。一条规则可以属于多个规则模板。

  入侵防御安全引擎提供自定义规则功能，通过对进入设备报文的协议类型，协议字段，字段内容形成匹配条件，并通过逻辑与、逻辑或形成多条件匹配的方式实现入侵防御。安全管理员可以使用自定义规则功能，自己写签名进行防护。自定义规则检测是基于流检测的，支持多种协议字段，其中包括 IP、UDP、TCP、FTP、HTTP、ICMP、POP3、SMTP 协议。对于字符串字段，可支持正则和非正则匹配的方式。

入侵防御的配置思路：

(1) 配置规则模板，决定需要对哪些事件做检测，并决定检测到攻击之后的日志和动作，可以使用系统预定义的规则模板，也可以自定义新的规则模板。

(2) 配置安全控制策略，在安全控制策略中配置入侵防御策略，引用已经配置的规则模板，对命中安全策略的流量做入侵防御相关的检测。

1.2 入侵防御规则模板配置

1.2.1 规则模板页面

通过菜单“策略配置>安全设置>入侵防御>模板”，进入如图 1-1 所示界面。可以查看系统预定义的规则模板和自定义的规则模板信息。

图1-1 入侵防御模板页面

在该页面上，默认显示所有入侵防御规则模板，同时能够“新建”、“编辑”、“删除”、“派生”规则模板。

1.2.2 新建规则模板

在模板页面点击“新建”，系统弹出新建规则模板对话框，如图 1-2 所示。入侵防御规则模板配置信息如表 1-1 所示。

图1-2 新建入侵防御规则模板

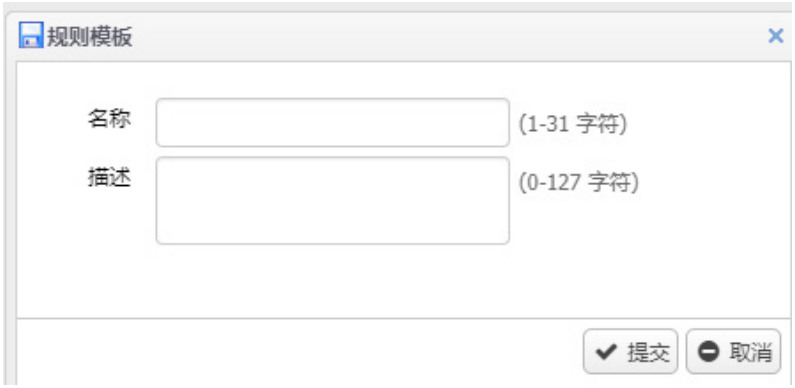


表1-1 新建入侵防御规则模板说明

参数	说明
名称	规则模板的名称，可输入1-31个字符，且不能与已创建的规则模板名称重复。
描述	规则模板的描述信息

输入完名称、描述之后，点击提交，完成规则模板的创建。

在规则模板页面点击需要修改的模板后的“”，进入规则模板编辑页面，可以对描述信息进行编辑，规则模板的名称不可变更。

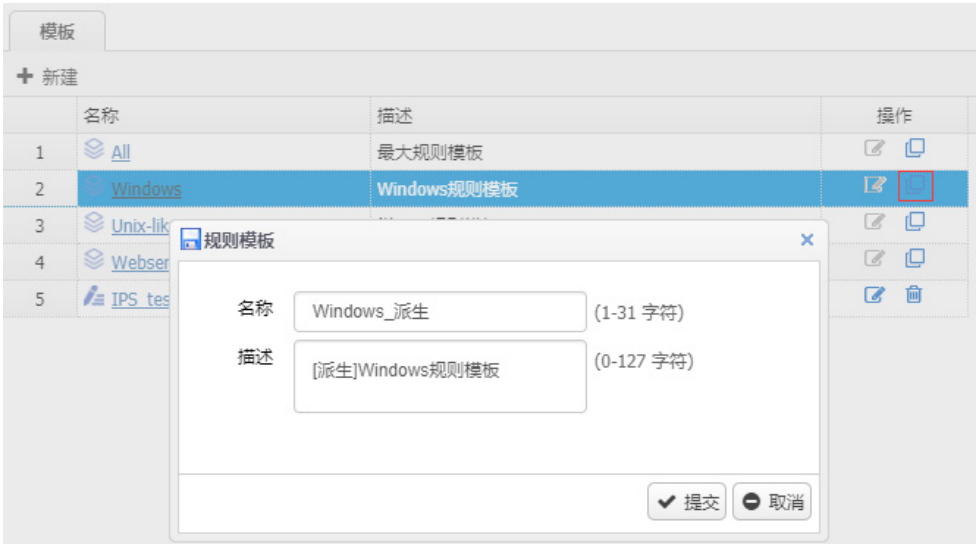
在入侵防御配置页面点击需要删除的规则模板后的“”，系统弹出确定对话框，点击“确定”后即可删除规则模板。

1.2.3 派生规则模板

用户可以根据已经存在的预定义规则模板，派生出相同的自定义规则模板。

点击模板后面的派生图标“”，进入规则模板对话框，如图 1-3 所示。

图1-3 派生 IPS 规则模板



输入新规则模板的名称、描述信息之后，就完成规则模板的派生。

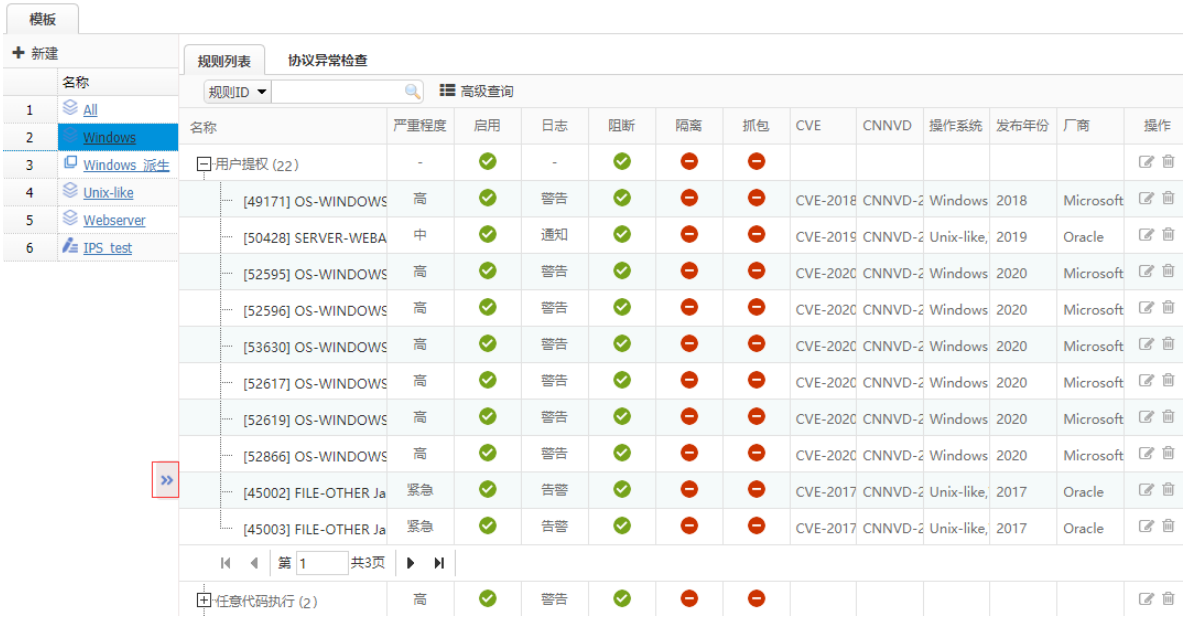
说明

- 派生后的规则模板不允许增加或删除，可以修改每条规则的配置。
- 派生规则模板不可以再派生。

1.2.4 查看规则列表

通过菜单“策略配置>安全设置>入侵防御>规则”进入入侵防御规则模板界面，在规则模板列表中单击需要查看的规则模板名称，在右侧展开显示规则列表信息。如图 1-4 所示。

图1-4 显示规则列表



点击规则列表页面左侧的“»”按钮，可以返回到规则模板主页面。

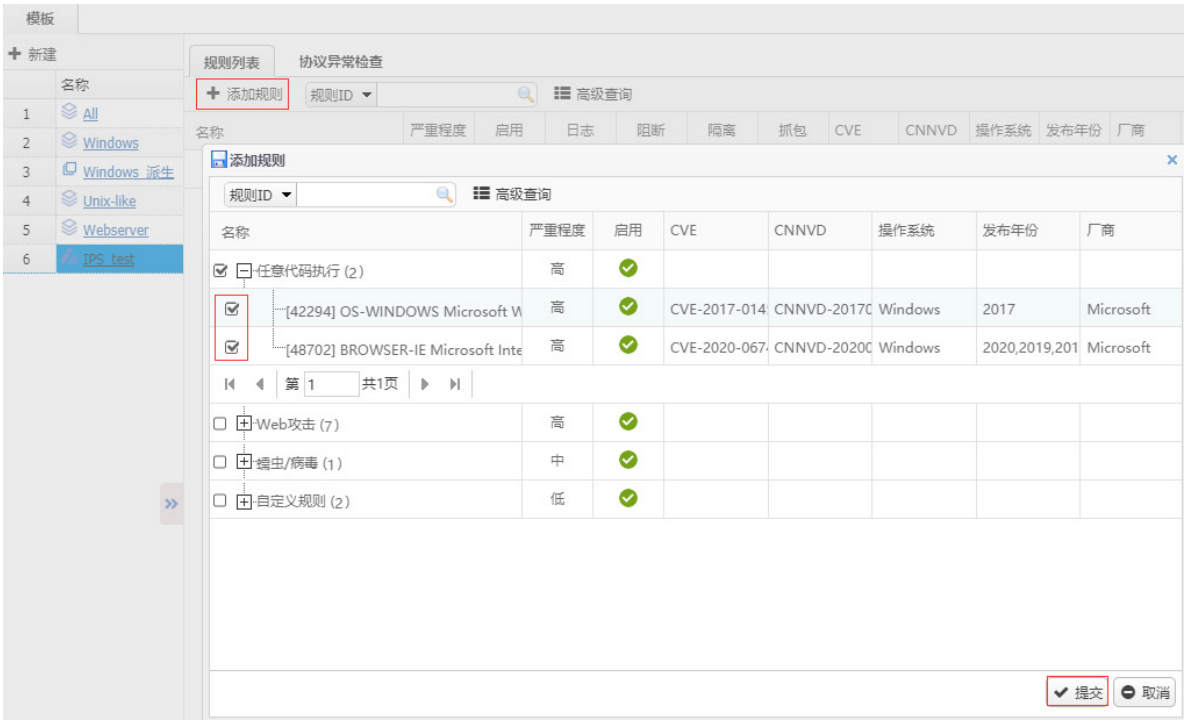
点击规则列表中的子规则名称，可以查看具体规则的详细信息，如下图所示。

图1-5 查看规则详细信息

1.2.5 添加规则

单击选择需要添加规则的自定义规则模板，进入规则列表页面，点击“添加规则”，弹出“添加规则”配置窗口，如图 1-6 所示。

图1-6 选择要添加的规则



勾选需要添加的规则后，点击“提交”，可以将选中的规则添加到对应的规则模板中。

点击规则后面的“”按钮，可以删除已添加的规则。

说明

只有自定义的规则模板可以添加、删除规则，预定义规则模板及派生后的规则模板不允许添加、删除规则。

1.2.6 修改规则配置

对于自定义的规则模板或者派生的规则模板，可以修改规则是否启用、是否记录日志，及阻断、隔离、抓包等配置。

(1) 通过菜单“策略配置>安全设置>入侵防御>模板”进入入侵防御规则模板界面，单击选择自定义规则模板，展开显示规则列表，如图 1-7 所示。

图1-7 展开规则列表

(2) 选择要编辑的规则，点击编辑按钮，弹出规则列表的编辑界面，如图 1-8 所示，各个配置项含义如表 1-2 所示。

图1-8 规则列表编辑页面

表1-2 编辑规则配置项含义描述表

参数	说明
启用	开启或关闭该事件
日志	该规则的日志是否记录及日志级别，可以配置成不记录或告警、警告、通知、信息。
阻断	是否阻断，如果配置为阻断，则匹配到规则后对数据报文或流进行丢弃处理。
隔离	是否隔离，如果配置为隔离，则匹配到规则后进行隔离处理：会将报文的源地址加入黑名单，隔离时间到期后解除隔离。
抓包	是否抓包，如果配置为抓包，则匹配到规则后进行抓包处理，在IPS日志页面可以下载抓包文件进行查看。

(3) 点击提交，完成规则配置的编辑。

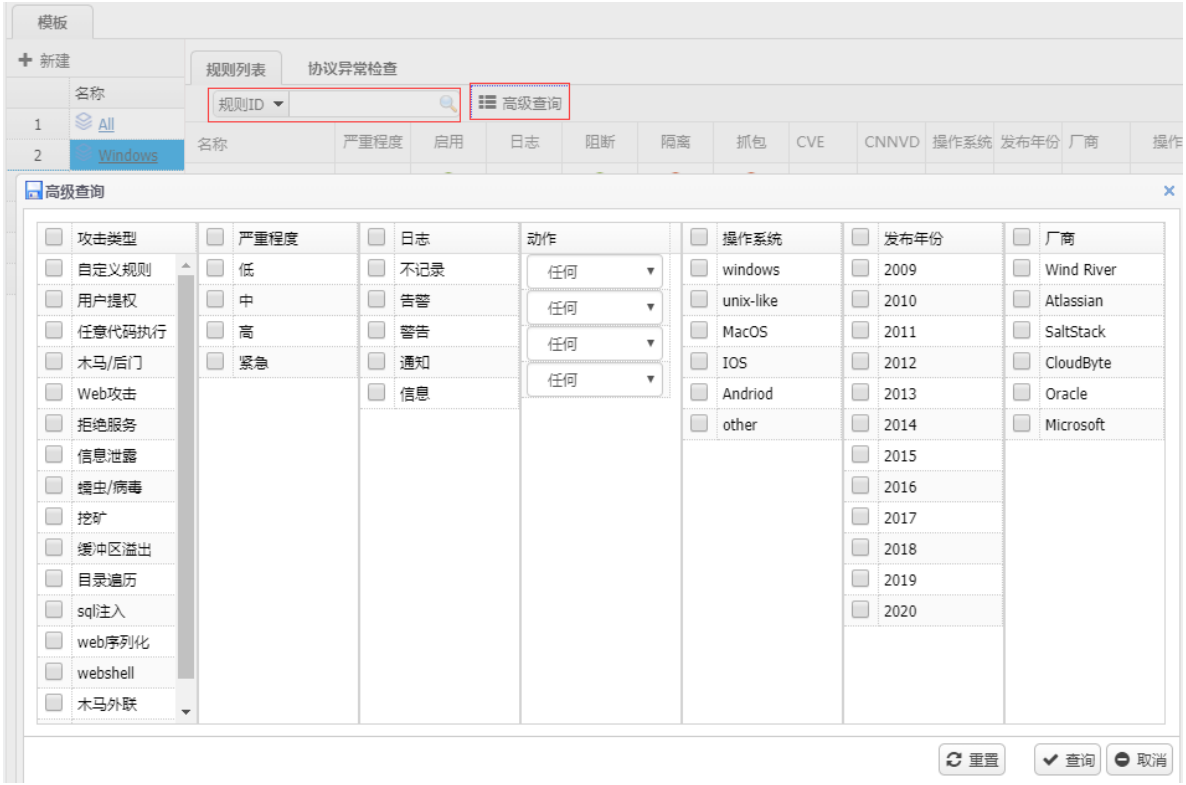
注意

只能对自定义规则模板及派生规则模板中的规则配置进行编辑，系统预定义规则中的内容无法编辑。

1.2.7 查询事件

可以根据规则 ID、名称、CVE、CNNVD 对规则模板中的规则进行查询，也可以点击“高级查询”，进入高级查询页面，选择攻击类型、严重程度、日志、动作、操作系统等查询条件进行查询。

图1-9 选定事件集



1.3 入侵防御协议异常检测

1.3.1 协议异常检测简介

安全策略通过对进入设备报文的协议类型，协议字段，字段内容形成匹配条件，并通过逻辑与和逻辑或形成多条件匹配的方式实现入侵防御。

1.3.2 协议异常检查页面

在导航栏中选择“策略配置>安全设置>入侵防御>模板”，进入 IPS 模板界面，点击模板名称选择协议异常检测页面，如下图所示。

图1-10 图 1-10 IPS 协议异常检查界面

IPS 协议检查说明，如表 1-9 所示。

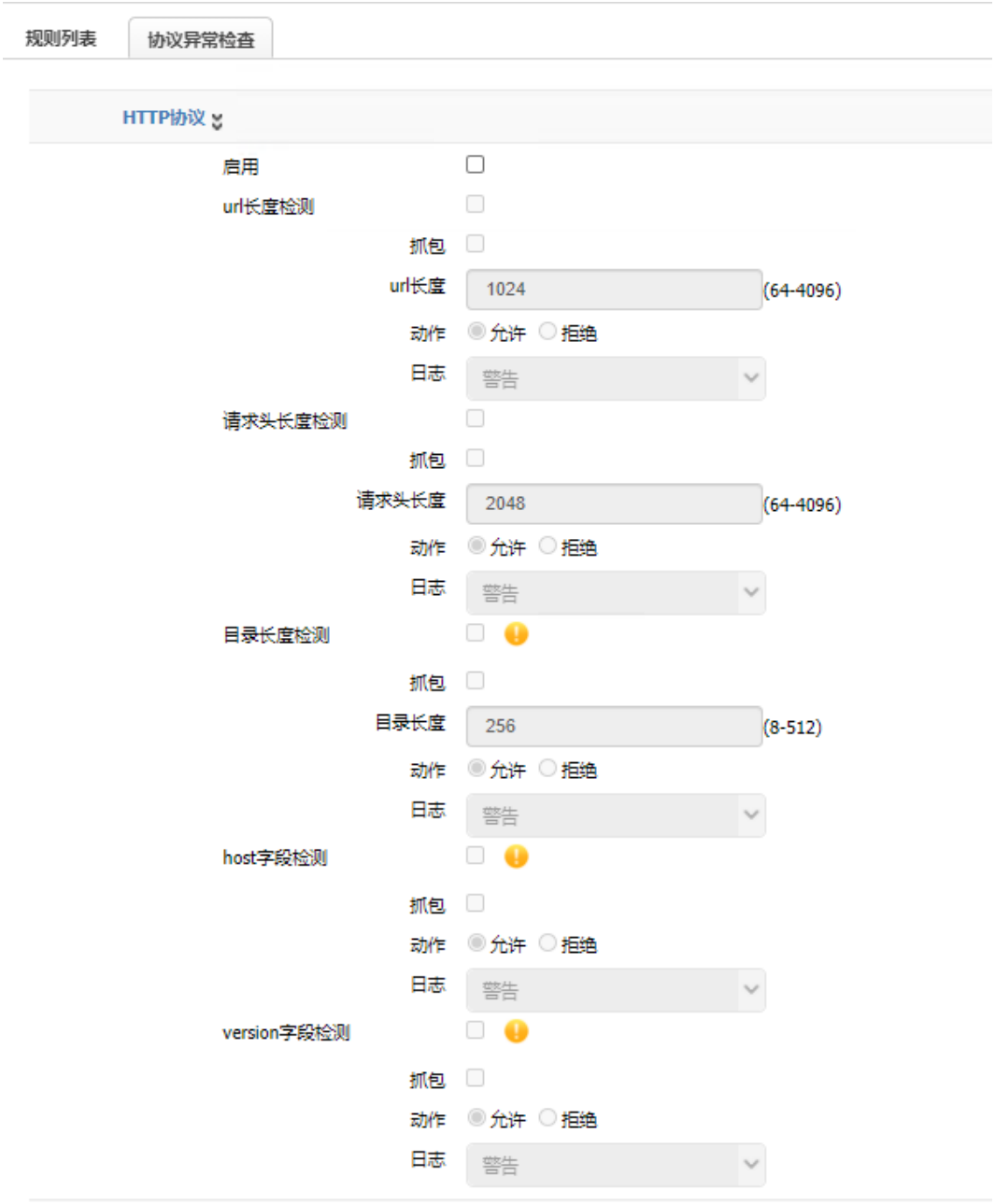
表1-3 IPS 异常检查描述表

标题项	说明
HTTP协议	针对HTTP协议字段进行检测，支持检测HTTP头版本字段，host字段，头长度，响应数据格式字段，并提供配置选项。
DNS协议	检测协议响应类型异常，域名长度，域名异常字符。
SMTP协议	根据配置检测命令参数长度，并提供手动配置与默认配置。
POP3协议	检测协议的命令行最大长度，文本行最大长度，内容文件名最大长度，并提供手动配置与默认配置。
FTP协议	检测协议的命令行最大长度，文本行最大长度，内容文件名最大长度，并提供手动配置与默认配置。

1.3.3 HTTP 协议异常检查

在导航栏中选择“策略配置>安全设置>入侵防御>模板”，进入 IPS 模板界面，点击模板名称选择协议异常检测页面，进入 HTTP 协议配置页面，如下图所示。

图1-11 HTTP 协议异常检查界面



HTTP 协议检查说明，如下表所示。

表1-4 HTTP 异常检查描述表

标题项	说明
协议异常检测启用	协议检查总开关
HTTP URL长度检测	勾选启用
url 长度	启用url长度检测
抓包	开启抓包

标题项	说明
url 长度	url长度范围为：64-4096
动作	允许/拒绝
日志	日志级别配置
请求头长度检测	勾选启用
抓包	开启抓包
请求头长度	请求头长度范围为：64-4096
动作	允许/拒绝
日志	日志级别配置
目录长度检测	勾选启用
抓包	开启抓包
目录长度	目录长度范围为：8-512
动作	允许/拒绝
日志	日志级别配置
Host字段检测	勾选启用
抓包	开启抓包
动作	允许/拒绝
日志	日志级别配置
Version字段检测	勾选启用
抓包	开启抓包
动作	允许/拒绝
日志	日志级别配置

1.3.4 DNS 协议异常检查

在导航栏中选择“策略配置>安全设置>入侵防御>模板”，进入 IPS 模板界面，点击模板名称选择协议异常检测页面，进入 DNS 协议配置页面，如下图所示。

图1-12 DNS 协议异常检查界面

DNS 协议检查说明，如下表所示。

表1-5 DNS 异常检查描述表

标题项	说明
启用	勾选启用DNS协议检查
域名长度检测	勾选启用DNS域名长度检测
抓包	开启抓包
域名长度	域名长度范围为：1-1024
动作	允许/拒绝
日志	日志级别配置
域名字符检测	勾选启用
抓包	开启抓包
动作	允许/拒绝
日志	日志级别配置

1.3.5 SMTP 协议异常检查

在导航栏中选择“策略配置>安全设置>入侵防御>模板”，进入 IPS 模板界面，点击模板名称选择协议异常检测页面，进入 SMTP 协议配置页面，如下图所示。

图1-13 SMTP 协议异常检查界面

SMTP 协议检查说明，如下表所示。

表1-6 SMTP 异常检查描述表

标题项	说明
启用	勾选启用SMTP协议检查
文本长度检测	勾选启用SMTP文本长度检测
抓包	开启抓包
文本行长度	文本行长度范围为：64-2048
动作	允许/拒绝
日志	日志级别配置
附件文件名长度检测	勾选启用
抓包	开启抓包
附件文件名长度	附件文件名长度范围为：1-512
动作	允许/拒绝
日志	日志级别配置

1.3.6 POP3 协议异常检查

在导航栏中选择“策略配置>安全设置>入侵防御>模板”，进入 IPS 模板界面，点击模板名称选择协议异常检测页面，进入 POP3 协议配置页面，如下图所示。

图1-14 POP3 协议异常检查界面

POP3 协议检查说明，如下表所示。

表1-7 POP3 异常检查描述表

标题项	说明
启用	勾选启用POP3协议检查
文本长度检测	勾选启用POP3文本长度检测
抓包	开启抓包
文本行长度	文本行长度范围为：64-2048
动作	允许/拒绝
日志	日志级别配置
附件文件名长度检测	勾选启用
抓包	开启抓包
附件文件名长度	附件文件名长度范围为：1-512
动作	允许/拒绝
日志	日志级别配置

1.3.7 FTP 协议异常检查

在导航栏中选择“策略配置>安全设置>入侵防御>模板”，进入 IPS 模板界面，点击模板名称选择协议异常检测页面，进入 FTP 协议配置页面，如下图所示。

图1-15 FTP 协议异常检查界面

FTP 协议检查说明，如下表所示。

表1-8 FTP 异常检查描述表

标题项	说明
启用	勾选启用FTP协议检查
命令行长度检测	勾选启用FTP命令行长度检测
抓包	开启抓包
命令行长度	命令行长度范围为：2-128
动作	允许/拒绝
日志	日志级别配置
命令参数长度检测	勾选启用
抓包	开启抓包

标题项	说明
命令参数长度	命令参数长度范围为：2-1024
动作	允许/拒绝
日志	日志级别配置

1.4 入侵防御自定义规则

1.4.1 入侵防御自定义规则简介

安全策略通过对进入设备报文的协议类型，协议字段，字段内容形成匹配条件，并通过逻辑与和逻辑或形成多条件匹配的方式实现入侵防御。

1.4.2 入侵防御规则库显示

在导航栏中选择“策略配置>安全设置>入侵防御>规则库”，进入 IPS 规则库界面，可以查看规则库的规则信息，包括系统预定义规则及用户自定义规则信息，如图 1-16 所示。

图1-16 IPS 规则库显示界面

1.4.3 入侵防御自定义规则配置

在入侵防御规则库页面，点击<添加自定义规则>进入 IPS 自定义规则配置页面，如图 1-17 所示。

图1-17 自定义规则配置页面图

IPS 自定义规则详细配置说明，如表 1-9 所示。

表1-9 自定义规则配置页面信息描述表

标题项	说明
名称	自定义规则的名称
严重程度	规则的严重程度，分为：低、中、高、紧急，根据规则的严重程度确定日志的级别。
方向	规则检测的方向：双向检测、向客户端、向服务端。
协议字段	每个协议字段可以包含8个协议匹配条件，每个匹配条件间为逻辑或。 每条自定义规则可以包含8个协议字段，协议字段之间为逻辑与。 匹配时先匹配每个字段的匹配条件或进行协议字间匹配,即先或后与 表达式为 (..&&..)|||(..&&..)。

1.4.4 协议字段的配置

在入侵防御自定义规则显示页面，点击<新建自定义规则>可以进入自定义规则配置页面，可以选择多种协议以及协议字段，配置字段详细信息如表 1-10 所示

表1-10 协议字段配置方式对应表

协议类型	协议字段	配置方式
IP	协议	● 等于 ● 不等于
	负载长度	● 等于 ● 大于 ● 小于

协议类型	协议字段	配置方式
	负载	包含
UDP	源端口号	● 等于 ● 不等于 ● 大于
	目的端口号	● 等于 ● 不等于 ● 大于
	负载长度	● 等于 ● 大于 ● 小于
	负载	包含
TCP	源端口号	● 等于 ● 不等于 ● 大于
	目的端口号	● 等于 ● 不等于 ● 大于
	负载长度	● 等于 ● 大于 ● 小于
	负载	包含
ICMP	类型	● 等于 ● 不等于 ● 大于
	代码	● 等于 ● 不等于 ● 大于
	负载长度	● 等于 ● 大于 ● 小于
	负载	● 包含 ● 正则匹配
HTTP	方法内容	● 等于 ● 不等于
	URL内容	● 包含 ● 正则匹配

协议类型	协议字段	配置方式
	HOST内容	● 包含 ● 正则匹配
	Cookie内容	● 包含 ● 正则匹配
	Header内容	● 包含 ● 正则匹配
	User-Agent内容	● 包含 ● 正则匹配
	方法长度	● 等于 ● 大于 ● 小于
	版本长度	● 等于 ● 大于 ● 小于
	URL长度	● 等于 ● 大于 ● 小于
	HOST长度	● 等于 ● 大于 ● 小于
	Cookie长度	● 等于 ● 大于 ● 小于
	Header长度	● 等于 ● 大于 ● 小于
	User-Agent长度	● 等于 ● 大于 ● 小于
FTP	命令内容 ftp标准命令如：STOR,RETR,MLSD	● 包含 ● 正则匹配
	命令参数内容 命令后面跟的参数如 RETR <文件名>	● 包含 ● 正则匹配
	命令长度	● 等于 ● 大于 ● 小于

协议类型	协议字段	配置方式
	命令参数长度	● 等于 ● 大于 ● 小于
POP3	命令内容 POP3命令如：user	● 包含 ● 正则匹配
	命令参数内容	● 包含 ● 正则匹配
	命令长度	● 等于 ● 大于 ● 小于
	命令参数长度	● 等于 ● 大于 ● 小于
SMTP	命令内容 SMTP命令如：mail	● 包含 ● 正则匹配
	命令参数内容	● 包含 ● 正则匹配
	命令长度	● 等于 ● 大于 ● 小于
	命令参数长度	● 等于 ● 大于 ● 小于

1.5 入侵防御防逃避

1.5.1 入侵防御防逃避简介

在 IPS 实际的使用场景中，攻击者往往会使用逃避技术来掩盖攻击，从而避免被 IPS 设备发现。如果安全产品未能识别出逃避行为，本来能够防护的漏洞就会轻易被绕过，鉴于此设备增加了 IPS 防逃避能力，提高对 IPS 逃避行为的检测能力。此功能只有进入 IPS 流程后，才能进入 IPS 防逃避流程。

目前支持 FTP 防逃避、URL 防逃避、HTML 防逃避检测，只支持命令行。

1.5.2 入侵防御防逃避 命令行

IPS 防逃避命令参数配置说明，如下表所示。

表1-11 IPS 防逃避命令参数配置

【命令名称】	**ips normalize { all | http_header | http_post_form | http_javascript | http_utf_file }**
【视图】	配置视图
【描述】	配置使能IPS防逃避功能需要正规化的字段 默认状态均为关闭
【参数解释】	**http_header**：HTTP头部字段； **http_post_form**：http_post_form_data字段（请求方向的http_msgbody）； **http_javascript**：HTTP响应的JS文件； **http_utf_file**：HTTP响应的文件（UTF16或UTF32编码）。
【命令名称】	**no ips normalize { all | http_header | http_post_form | http_javascript | http_utf_file }**
【视图】	配置视图
【描述】	配置关闭IPS防逃避功能需要正规化的字段

1.6 入侵防御策略

如需使入侵防御生效，必须在相应的安全策略上面启用入侵防御策略。

通过菜单“策略配置>控制策略”进入控制策略界面，新建或者编辑一条已经存在的策略；点击“入侵防御”标签页，进入“入侵防御”配置界面，如图 1-18 所示。各个配置项含义如表 1-12 所示。

图1-18 入侵防御策略

表1-12 入侵防御策略配置项含义描述表

参数	说明
规则模板	选择入侵防御使用的规则模板名称
防护模式	是否启用防护模式，只有启用防护模式且模板下的规则或协议异常检查配置为阻断，匹配到策略后才会阻断流量。

说明

- R6612 及以上版本中，入侵防御预定义规则模板的默认动作为阻断，匹配到规则后会对数据报文或流进行丢弃处理。因此，开局时如果使用预定义模板规则，建议取消勾选“防护模式”，系统运行一段时间后，再根据实际场景情况定义合适的入侵防御规则模板。
- 设备从 R6612 以下版本升级到 R6612 及以上版本时，除了 IPS 自定义规则，其它所有 IPS 配置不进行恢复，如果原来控制策略中配置了 IPS 策略，则默认恢复为引用 All 模板的 IPS 策略。升级后，建议将 IPS 策略的“防护模式”设置为不勾选，系统运行一段时间后，再根据实际场景情况定义合适的入侵防御规则模板。

1.7 入侵日志聚合

IPS 入侵日志支持聚合，系统可将符合聚合规则（协议 ID 相同、特征规则 ID 相同）的日志信息进行聚合，从而减少日志数量，避免日志服务器接受冗余的日志信息。系统仅支持聚合由 IPS 功能所产生的日志信息。聚合的前提条件是特征规则 ID、应用必须相同，然后根据聚合方式进行聚合。该功能默认为关闭状态。

通过菜单“数据中心>日志中心>安全日志>入侵日志>日志聚合”进入日志聚合配置界面，点击“下拉框”选择日志聚合方式，如图 1-18 所示。各个配置项含义如表 1-12 所示。

图1-19 入侵防御日志聚合

表1-13 入侵防御日志聚合方式配置项含义描述表

聚合方式	说明
不聚合	默认不聚合

聚合方式	说明
按照规则聚合	是指一段时间之内相同规则ID、相同应用的事件只会产生一条日志。
按源IP聚合	是指一段时间之内相同源IP、相同规则ID、相同应用的事件只会产生一条日志。
按目的IP聚合	是指一段时间之内相同目的IP、相同规则ID、相同应用的事件只会产生一条日志。
按源目IP聚合	是指一段时间之内相同源IP、相同目的IP、相同规则ID、相同应用的事件只会产生一条日志。

1.8 入侵日志告警规则

通过菜单“数据中心>日志中心>安全日志>入侵日志>告警规则”进入告警规则配置界面，点击“新建”进入告警规则配置页面，如下图所示。

图1-20 入侵防御告警规则

表1-14 入侵防御告警规则配置项含义描述表

参数	说明
规则名称	告警规则名称，可输入1-31个字符，不支持中文。
源地址	源地址对象支持子网、范围、主机地址三种。
目的地址	目的地址对象支持子网、范围、主机地址三种。
代理地址	代理地址对象：支持子网、范围、主机地址三种。

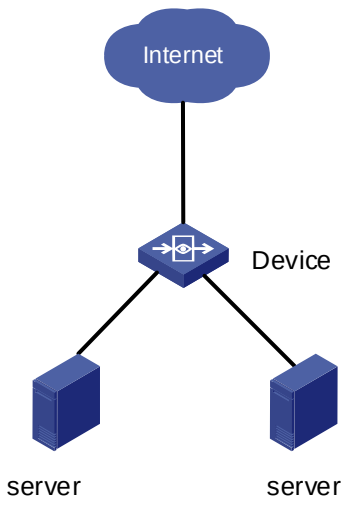
参数	说明
源端口	范围为：0-65535，0代表任意端口。
目的端口	范围为：0-65535，0代表任意端口。
级别	全部、告警、严重、警告、通知、信息。
动作	全部、允许、拒绝、丢弃、丢弃会话、阻断源地址。
事件类型	全部、CGI攻击、安全审计、木马后门、CGI访问、可疑行为、安全漏洞、缓冲溢出、拒绝服务、蠕虫病毒、间谍软件、安全扫描、网络娱乐、协议分析、网络数据库攻击、网络设备攻击、欺骗劫持、分布式拒绝服务、网络通讯、脆弱口令、穷举检测、WAF攻击。
发送频率	时间范围（60-86400秒），攻击条数阈值（1~99999999）。
外发设置	syslog， 邮件（配置邮箱）。
告警邮件	收件地址：多个邮箱回车分割，最多支持输入32个。

1.9 入侵防御配置举例

1.9.1 组网需求

如图 1-21 所示，服务器通过 Internet 提供 web 和 FTP 服务，在设备上启用入侵防御功能来保护 Web 和 FTP 服务器。同时通过自定义规则来禁止使用除 210 以外的端口访问 ftp 服务器，且不允许上传文件和新建目录，为了减少日志量，按照规则进行日志聚合。

图1-21 入侵防御功能配置组网图



1.9.2 配置思路

- 配置模板，决定需要对哪些规则做检测，并决定检测到攻击之后的日志和动作，可以使用系统预定义的模板，也可以自定义新的模板。

- 配置控制策略，在控制策略中配置入侵防御，引用已经配置的模板，对命中控制策略的流量做入侵防御相关的检测。

1.9.3 配置注意事项

- 入侵防御策略匹配是由上至下进行匹配，策略匹配到之后将不会往下继续匹配。
- 是否启用防护模式，只有启用防护模式且模板下的规则或协议异常检查配置为阻断，匹配到策略后才会阻断流量。

1.9.4 配置步骤

1. 配置自定义入侵防御规则

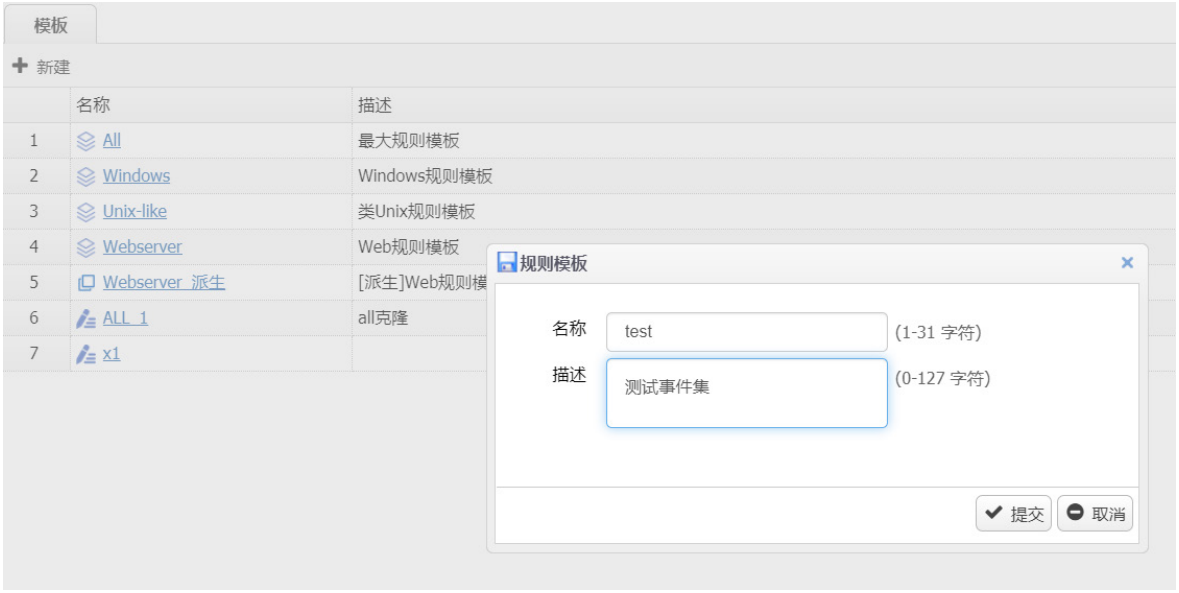
进入“策略配置>安全设置>入侵防御>规则库”，进入 IPS 自定义规则配置页面，如下图所示，禁止使用除 210 以外的端口访问 ftp 服务器，且不允许上传文件和新建目录。

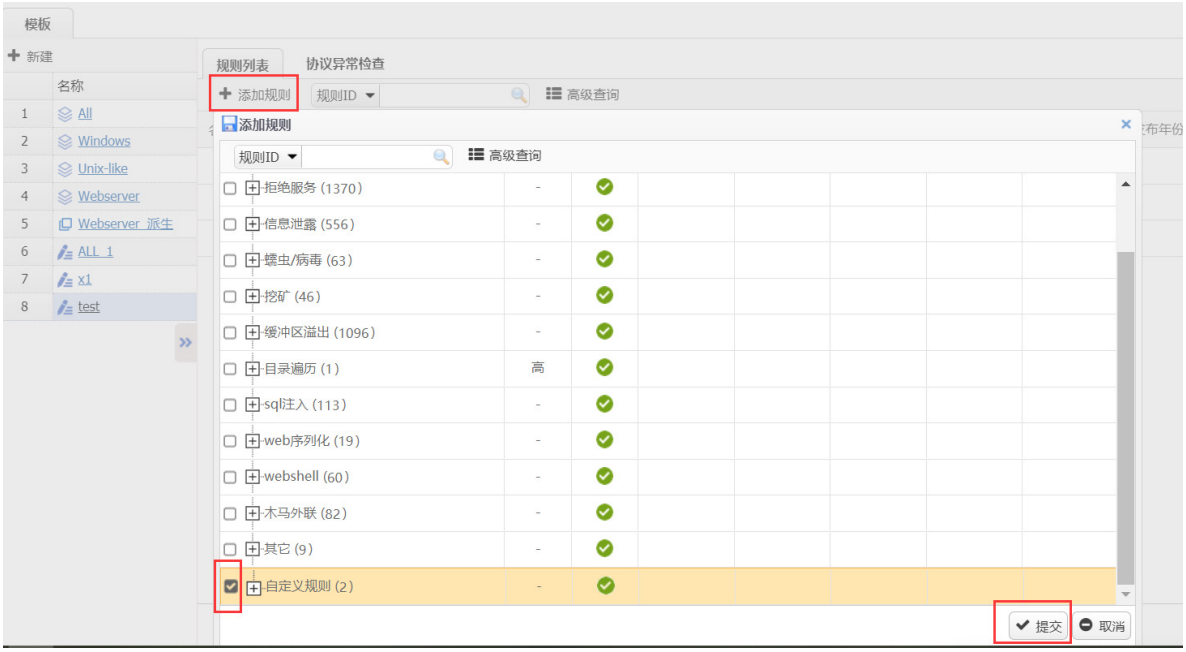
图1-22 配置自定义入侵防御规则

2. 配置入侵防御模板

进入“策略设置>安全设置>入侵防御>模板”，进入入侵防御配置页面，新建模板并添加规则，如下图所示。

图1-23 配置入侵防御模板





3. 配置控制策略

进入“策略配置>策略配置>控制策略”，进入控制策略页面，如图 1-24 所示，新建策略，在入侵防御子菜单中启用功能并选择模板“test”，完成后点击提交。

图1-24 配置控制策略

4. 配置日志聚合

进入“数据中心>日志中心>安全日志>入侵日志>日志聚合”，进入日志聚合配置页面，如图 1-24 所示，选择聚合方式点击提交。

图1-25 配置日志聚合

1.9.5 验证配置

1. 默认入侵防御功能验证

使用测试 PC 进行攻击操作。在“数据中心>日志中心>安全日志>入侵日志”中可看到相应攻击日志信息，如图 1-26 所示。

图1-26 入侵日志

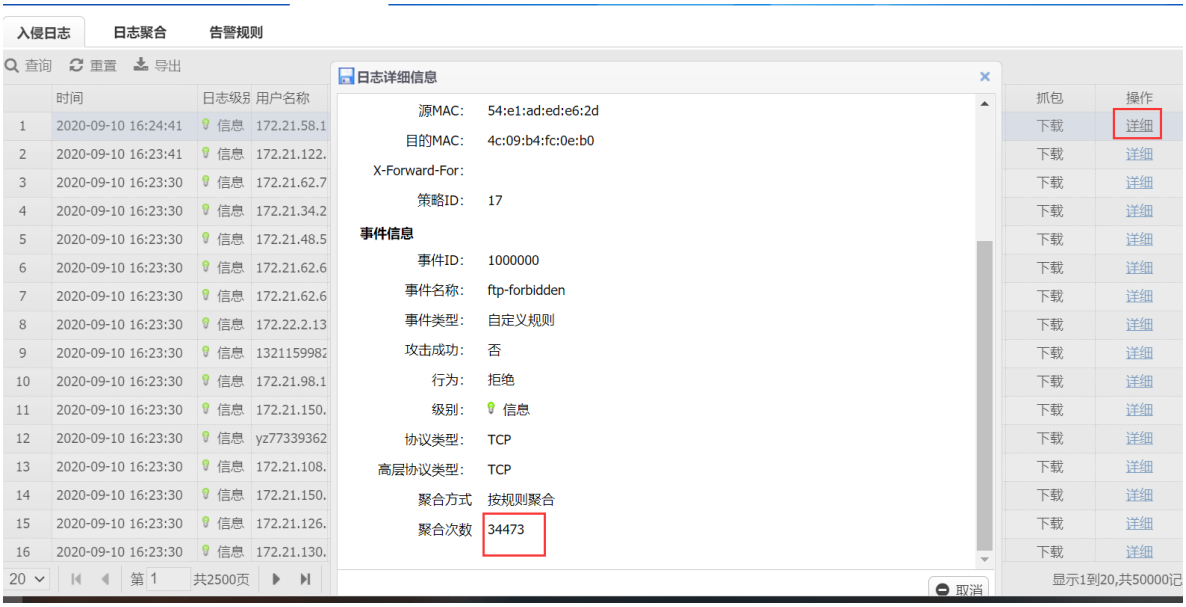
2. 自定义入侵防御功能验证

配置完成自定义 IPS 规则后，用户只能使用 210 端口访问 FTP 服务器，可以下载文件，但是无法上传和创建目录。否则无法登录服务器，并记录相应日志信息。使用测试 PC 进行 FTP 服务器登录操作，在“数据中心>日志中心>安全日志>入侵日志”中可看到相应日志信息，如图 1-27 所示。

图1-27 入侵检测日志

点击“详细”可看到相应日志的详细信息，包括日志聚合信息等，如图 1-27 所示。

图1-28 入侵检测日志聚合信息



目 录

1 病毒防护 ····· 1-1
1.1 病毒防护概述 ····· 1-1
1.2 防病毒设定 ····· 1-1
1.2.1 解压选项 ····· 1-1
1.2.2 新建扫描列表项 ····· 1-2
1.2.3 删除扫描列表项 ····· 1-2
1.2.4 启用禁用扫描列表项 ····· 1-2
1.3 病毒列表 ····· 1-3
1.4 病毒防护策略 ····· 1-4
1.5 配置案例 ····· 1-4
1.5.1 组网需求 ····· 1-4
1.5.2 配置步骤 ····· 1-5
1.5.3 验证配置 ····· 1-6

1 病毒防护

1.1 病毒防护概述

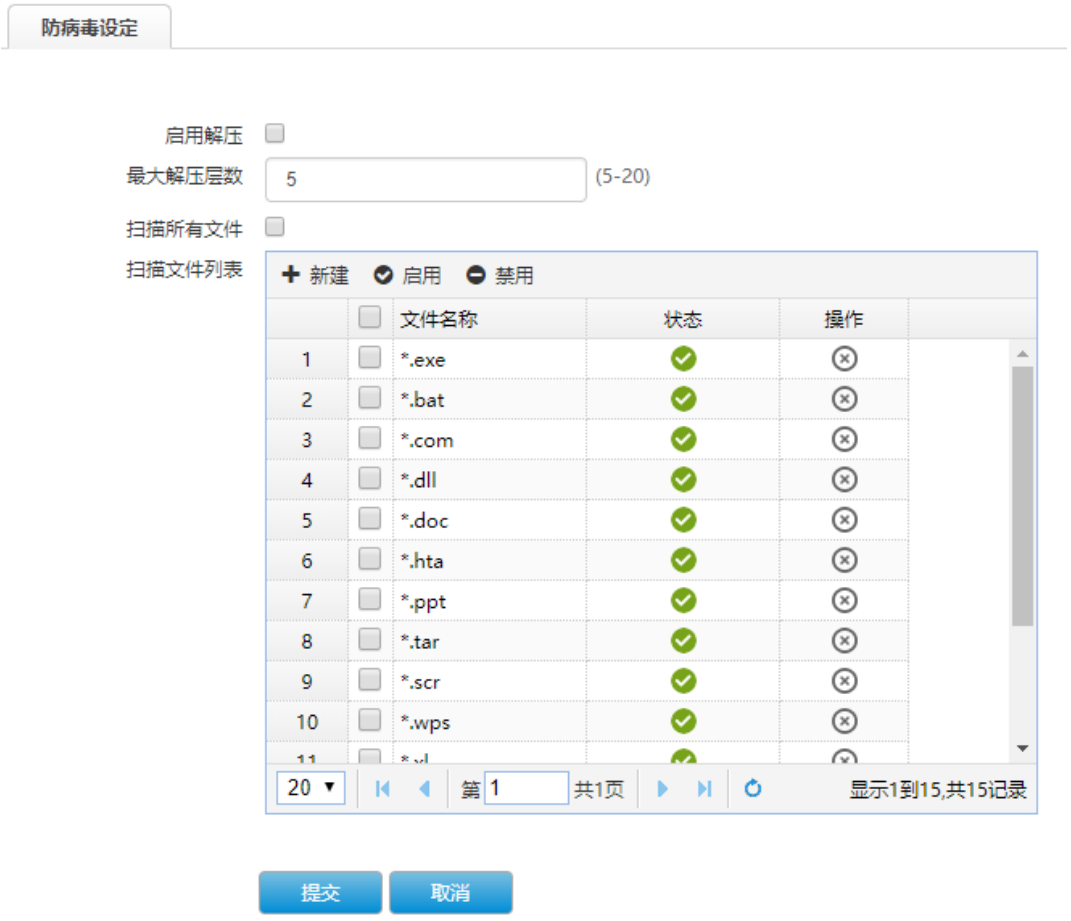
设备可以针对内外网入口处，进行实时的病毒扫描，将外来病毒隔离在内网之外，实现工作站被动防御病毒之外的主动病毒防护，我们可以在诸如 HTTP、FTP、IMAP、POP3、SMTP 等应用协议时进行文件扫描。

1.2 防病毒设定

通过菜单“策略配置 > 安全设置 > 病毒防护 > 防病毒设定”使用该功能。

1.2.1 解压选项

图1-1 防病毒设定

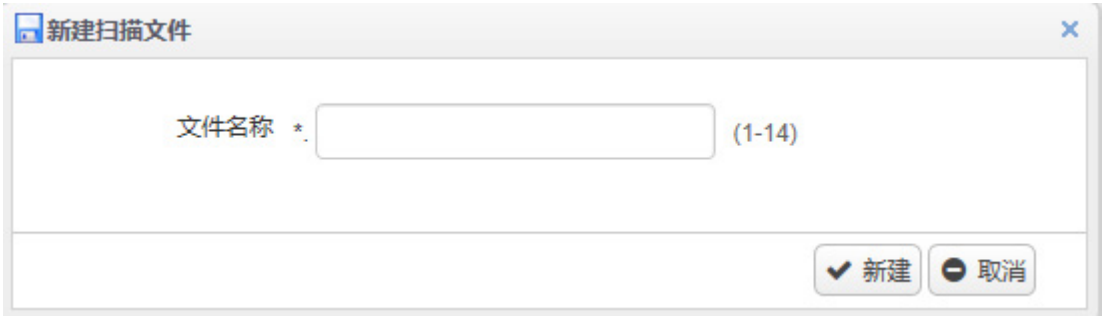


通过勾选启用解压按钮来启用解压功能，设置最大解压层数的值来设置解压过程中允许解压的最大层数。

1.2.2 新建扫描列表项

点击扫描文件列表后面的新建按钮，弹出新建扫描文件对话框，可以添加新的需要扫描的文件类型。

图1-2 新建扫描列表项



输入需要扫描的文件的后缀名。比如 txt 后，点击新建，可以增加扫描文件类型，会对文件后缀为.txt 文件进行病毒扫描。

1.2.3 删除扫描列表项

点击文件名称后面的删除按钮 ⊗，点击确定后即可删除对应的扫描列表项。

注意

只能删除用户自定义的扫描列表项，预自定的扫描列表项无法删除。

1.2.4 启用禁用扫描列表项

选中需要启用、禁用的文件名称。再点击工具栏上面的启用、禁用按钮，在弹出的对话框中点击确定。就可以完成文件扫描列项的启动或者是禁用。

图1-3 启用禁用扫描列表项

1.3 病毒列表

进入“策略配置 > 安全设置 > 病毒防护 > 病毒列表”，可以显示系统支持的病毒列表。

图1-4 病毒列表

病毒列表

	病毒名称
1	Adware/0005.exe
2	Adware/0006.exe
3	Adware/0007.exe
4	Adware/0008.exe
5	Adware/0012.exe
6	Adware/0023.exe
7	Adware/0024.exe
8	Adware/0029.exe
9	Adware/0030.exe
10	Adware/0031.exe
11	Adware/0033.exe
12	Adware/0036.exe

1.4 病毒防护策略

要想使病毒防护生效，必须在相应的安全策略上面启用病毒防护策略。进入“策略配置>控制策略”，新建或者编辑一条已经存在的策略，如图 1-5 所示；点击“病毒防护”标签页，进入“病毒防护”配置界面；各个配置项含义如表 1-1 所示。

图1-5 病毒防护策略

表1-1 病毒防护策略配置项含义描述表

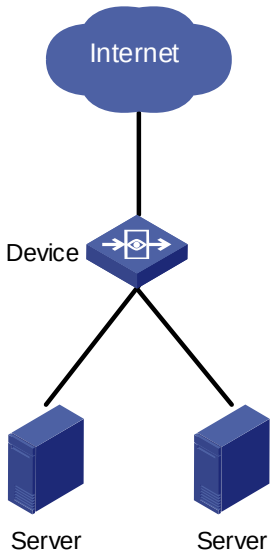
参数	说明
启用	启用或禁用病毒防护
日志	是否记录相关日志，勾选即为记录。
防护项目	HTTP、FTP、IMAP、POP3、SMTP是对应的协议类型，行为是对应的动作，有允许和阻断两种动作。

1.5 配置案例

1.5.1 组网需求

服务器通过 Internet 提供 web 和 FTP 服务，配置病毒防护策略来保护 Web 和 FTP 服务器。

图1-6 配置案例拓扑



1.5.2 配置步骤

(1) 编辑访问 internet 对应的控制策略，切换到病毒防护选项卡。

图1-7 配置病毒防护策略

(2) 勾选启用、日志。防护项目选中所有协议，行为选择阻断，点击确定，就可以完成病毒防护的配置。

1.5.3 验证配置

在导航栏中选择“数据中心>日志中心>安全日志>病毒防护日志”，进入病毒防护日志页面，可以查看到病毒防护日志信息

图1-8 病毒防护日志

目 录

1 安全防护 ····· 1-1
1.1 ARP/ND 攻击防护 ····· 1-1
1.1.1 ARP/ND 攻击防护概述 ····· 1-1
1.1.2 ARP 表项显示 ····· 1-1
1.1.3 ND 表项显示 ····· 1-1
1.1.4 ARP/ND Flood 攻击防护 ····· 1-2
1.1.5 防 ARP 欺骗 ····· 1-3
1.1.6 防 ND 欺骗 ····· 1-4
1.1.7 ARP/ND 学习控制 ····· 1-5
1.1.8 防 ARP 欺骗主动保护列表配置举例 ····· 1-6
1.1.9 防 ND 欺骗配置举例 ····· 1-7
1.2 异常报文攻击防护 ····· 1-10
1.2.1 异常报文攻击防护概述 ····· 1-10
1.2.2 异常报文攻击防护配置 ····· 1-11
1.2.3 异常报文攻击防护配置举例 ····· 1-12
1.3 IPv6 异常报文防护 ····· 1-13
1.3.1 IPv6 异常报文防护配置 ····· 1-13
1.3.2 IPv6 异常包攻击防护举例 ····· 1-14
1.4 扫描攻击防护 ····· 1-15
1.4.1 扫描攻击防护概述 ····· 1-15
1.4.2 扫描攻击防护配置 ····· 1-15
1.4.3 扫描攻击防护配置举例 ····· 1-16
1.5 DoS 攻击防护 ····· 1-18
1.5.1 DoS 攻击防护概述 ····· 1-18
1.5.2 目的 IP 防御设置 ····· 1-18
1.5.3 目的 IP 防御配置举例 ····· 1-19
1.5.4 接口防御设置 ····· 1-20
1.5.5 接口防御配置举例 ····· 1-22
1.6 IPMAC 绑定 ····· 1-22
1.6.1 IPMAC 概述 ····· 1-22
1.6.2 IPMAC 绑定添加 ····· 1-23
1.6.3 IPMAC 绑定配置举例 ····· 1-24
1.7 防 ARP 攻击 ····· 1-24

1.7.1 防 ARP 攻击概述 ····· 1-24
1.7.2 ARP 表项显示 ····· 1-25
1.7.3 ARP Flood 攻击防护 ····· 1-25
1.7.4 防 ARP 欺骗 ····· 1-26
1.7.5 主动保护列表添加 ····· 1-27
1.7.6 主动保护列表配置举例 ····· 1-27
1.8 行为模型 ····· 1-29
1.8.1 行为模型简介 ····· 1-29
1.8.2 行为模型配置页面 ····· 1-29
1.8.3 行为模型配置举例 ····· 1-31
1.9 防暴力破解 ····· 1-34
1.9.1 防暴力破解简介 ····· 1-34
1.9.2 防暴力破解配置 ····· 1-34
1.9.3 服务选择 ····· 1-35
1.10 弱密码防护 ····· 1-36
1.10.1 弱密码防护简介 ····· 1-36
1.10.2 弱密码防护 ····· 1-36
1.10.3 服务选择 ····· 1-37
1.10.4 弱密码规则 ····· 1-38
1.11 非法外联防护 ····· 1-39
1.11.1 非法外联防护简介 ····· 1-39
1.11.2 非法外联防护 ····· 1-40
1.11.3 非法外联学习 ····· 1-43

1 安全防护

1.1 ARP/ND攻击防护

1.1.1 ARP/ND 攻击防护概述

在 IPv4 局域网中，通过 ARP 协议将 IP 地址转换为 MAC 地址。ARP 协议对网络安全具有重要的意义，但是当初 ARP 方式的设计没有考虑到过多的安全问题，留下很多隐患，使得 ARP 攻击成为当前网络环境中遇到的一个非常典型的安全威胁。

在 IPv6 局域网中，通过 ND 协议将 IP 地址转换为 MAC 地址。由于 ND 协议并未提供认证机制，导致网络中的节点不可信，也使攻击者有机可乘，可针对 ND 协议发起一系列攻击。

通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量，使网络阻塞，攻击者只要持续不断的发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存，造成网络中断或中间人攻击。

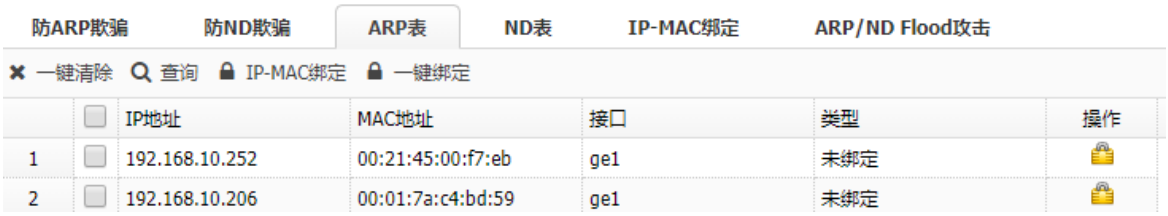
受到 ARP 攻击后会出现无法正常上网、ARP 包爆增、不正常或错误的 MAC 地址、一个 MAC 地址对应多个 IP、IP 冲突等情况。ARP 攻击因为技术门槛低，易于实现，在现今的网络中频频出现，有效防范 ARP 攻击已成为确保网络畅通的必要条件。

设备的防 ARP/ND 攻击功能有效识别 ARP/ND 欺骗攻击和 ARP/ND flood 攻击，对疑似攻击的行为告警，并配合 IP-MAC 绑定、主动保护发包及关闭 ARP/ND 学习等，有效防范 ARP/ND 攻击造成的损害。

1.1.2 ARP 表项显示

通过菜单“策略配置 > 安全设置 > 安全防护 > ARP/ND 防护 > ARP 表”进入 ARP 表显示界面，如下图所示。

图1-1 ARP 表项显示



1.1.3 ND 表项显示

通过菜单“策略配置 > 安全设置 > 安全防护 > ARP/ND 攻击防护 > ND 表”进入 ND 表显示界面，如下图所示。

图1-2 ND 表项显示

1.1.4 ARP/ND Flood 攻击防护

通过菜单“策略配置 > 安全设置 > 安全防护 > ARP/ND 攻击防护 > ARP/ND Flood 攻击”使用该功能，如下图所示。

图1-3 ARP/ND Flood 攻击设置页面

表1-1 ARP/ND Flood 攻击防护详细配置描述表

配置项	说明
启用防ARP flood	点选启用防ARP Flood攻击
ARP攻击识别阈值	一秒内收到ARP报文的数量，缺省配置为300个/秒。
ARP攻击主机抑制时长	设置阻断时间，当系统检测到攻击时，在配置的时长内拒绝来自于该台源主机的所有其它包，缺省配置为60秒。
启用防ND flood	点选启用防ND Flood攻击。
ND攻击识别阈值	一秒内收到ND报文的数量，缺省配置为300个/秒。
ND攻击主机抑制时长	设置阻断时间，当系统检测到攻击时，在配置的时长内拒绝来自于该台源主机的所有其它包，缺省配置为60秒。

1.1.5 防 ARP 欺骗

通过菜单“安全中心>其它防护>ARP/ND 攻击防护>防 ARP 欺骗”使用该功能。

图1-4 防 ARP 欺骗设置页面

表1-2 防 ARP 欺骗详细信息描述表

配置项	说明
关闭ARP学习	缺省情况下启用ARP学习，关闭后只要是不匹配IP-MAC绑定表的报文都将被丢弃
主动保护	点选启用主动保护发包功能，每隔一定时间间隔发送一次主动保护列表上的免费ARP报文
时间间隔	发送主动保护列表上的ARP的时间间隔，缺省配置为1秒

如图 1-4 所示，在防 ARP 欺骗设置页面中，选择主动保护列表下的<新建>按钮，将弹出如下页面。

图1-5 主动保护列表页面

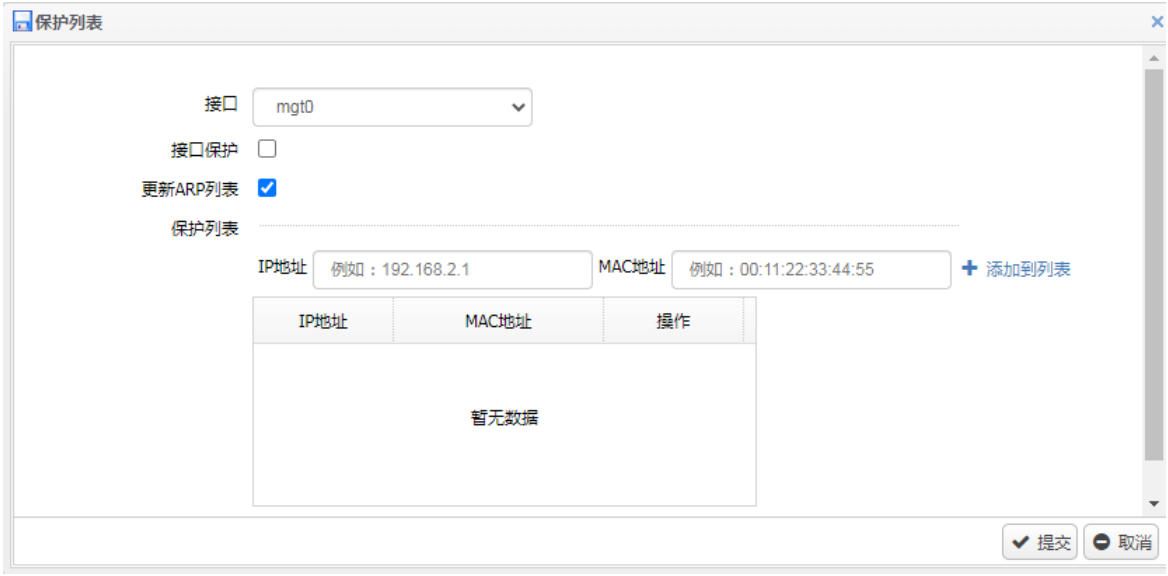


表1-3 主动保护详细信息描述表

配置项	说明
接口	ARP报文发送接口
接口保护	在保护列表中加入接口地址
IP地址&MAC地址	广播ARP报文的IP和MAC

1.1.6 防 ND 欺骗

如下图所示，通过菜单“安全中心>其它防护>ARP/ND 攻击防护>防 ND 欺骗”使用该功能。

图1-6 防 ND 欺骗设置页面

表1-4 防 ND 欺骗详细信息描述表

配置项	说明
关闭ND学习	缺省情况下启用ND学习，关闭后只要是不匹配IP-MAC绑定表的报文都将被丢弃
ND反向查询	点选启用或者不启用ND反向查询功能
IP地址数检查	每个MAC对应的IP地址的最大值，参数为0不检查，如果mac地址对应的IP地址数量多于设定值则产生告警
主动保护	点选启用主动保护发包功能，每隔一定时间间隔发送一次主动保护列表上的免费ARP报文
时间间隔	发送主动保护列表上的ND时间间隔，缺省配置为1秒

在防 ND 欺骗设置页面中，选择主动保护列表下的<新建>按钮，将弹出如下页面。

图1-7 主动保护列表页面

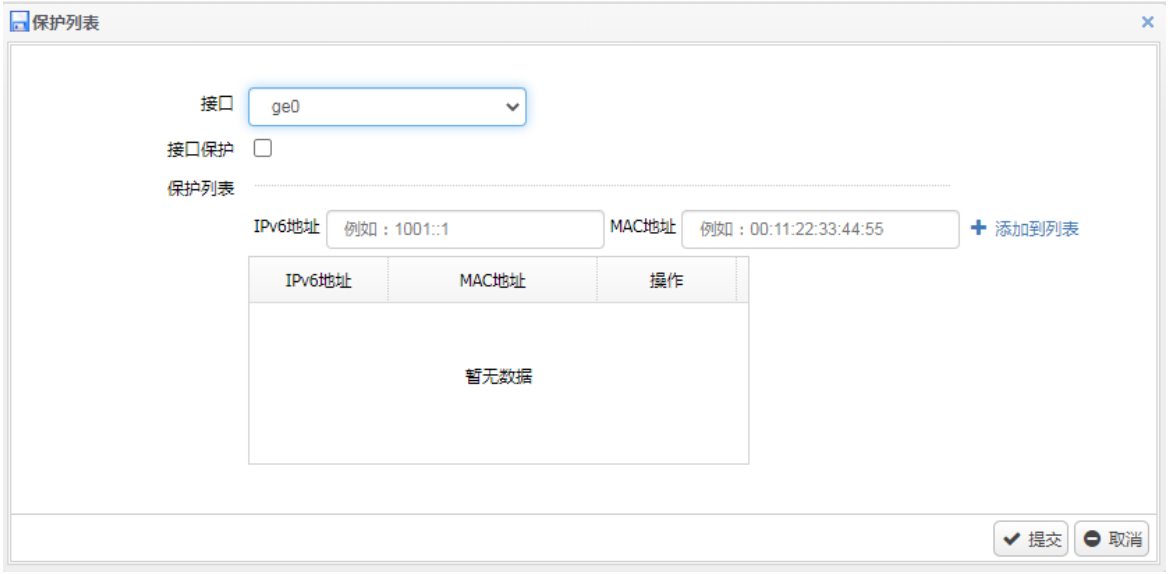


表1-5 主动保护详细信息描述表

配置项	说明
接口	ND报文发送接口
接口保护	在保护列表中加入接口地址
IP地址&MAC地址	ND报文的IP和MAC

1.1.7 ARP/ND 学习控制

如下图所示，通过菜单“策略配置 > 安全设置 > 安全防护 > ARP/ND 攻击防护 > ARP/ND 学习控制”使用该功能。

图1-8 ARP/ND 学习控制页面

如图图 1-8 所示，点击“新建”，进入接口的 ARP/ND 控制子页面。

图1-9 接口 ARP/ND 学习控制子页面

表1-6 接口 ARP/ND 学习控制子页面详细配置描述表

配置项	说明
接口	选择接口
ARP控制	启用或不启用ARP控制
ND控制	启用或不启用ND控制

1.1.8 防 ARP 欺骗主动保护列表配置举例

1. 用户需求

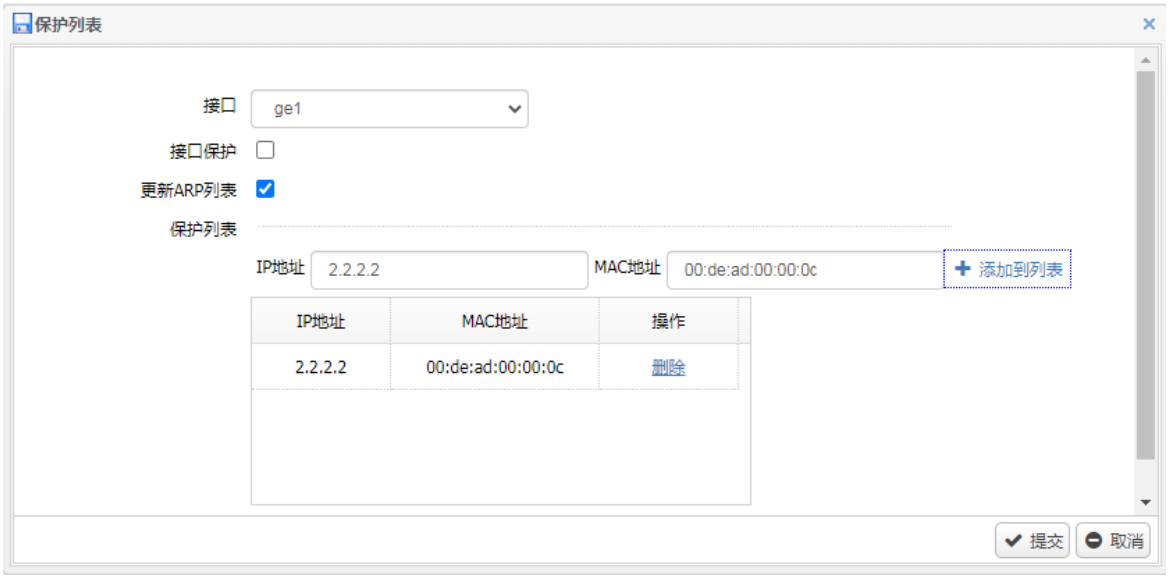
将接口 ge1 加入防 ARP 欺骗的主动保护列表中。保护的 IP 和 MAC 分别为：2.2.2.2 和 00:de:ad:00:00:0c。

2. 配置步骤

(1) 进入“安全中心>其它防护>ARP/ND 攻击防护>防 ARP 欺骗”，点击主动保护列表下面的<新建>按钮，进入主动保护列表配置页面

(2) 选择接口为 ge1，输入要保护的 IP 和 MAC 地址，点击“添加到列表”。

图1-10 主动保护列表配置页面



(3) 点击<提交>按钮后，可以在防 ARP 欺骗页面看到已添加的主动保护列表信息。

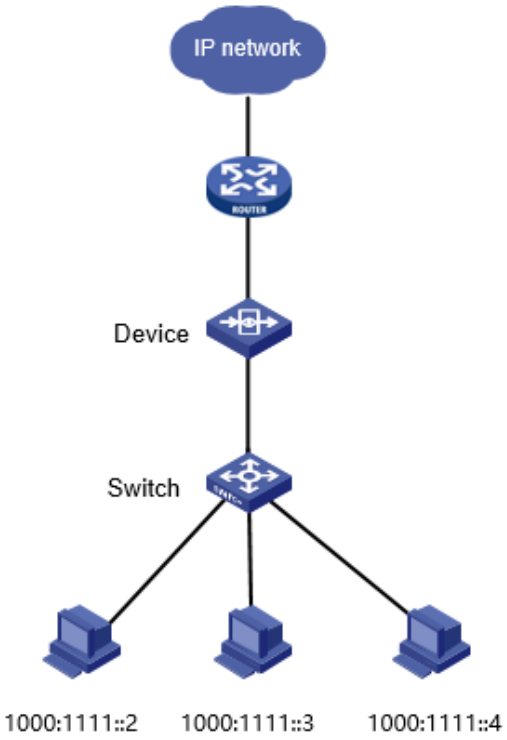
图1-11 防 ARP 欺骗页面

1.1.9 防 ND 欺骗配置举例

1. 组网需求

如下图所示，公司内网有多台服务器设备，防止服务器被局域网内 PC 进行 ND 欺骗造成服务器无法正常访问。

图1-12 防 ND 欺骗配置举例组网图



2. 配置步骤

(1) 进入“策略配置 > 安全设置 > 安全防护 > ARP/ND 攻击防护 > 防 ND 欺骗”；关闭 ND 学习，开启 ND 反向查询，设置每 MAC 地址 IP 数检查，开启接口主动保护，然后点击提交按钮提交配置。

图1-13 防 ND 欺骗配置

图1-14 启用防 ND 欺骗

进入“策略配置 > 安全设置 > 安全防护 > ARP/ND 攻击防护 > IP-MAC 绑定”；绑定被保护服务器的 IPMAC 地址，勾选唯一性，然后点击提交按钮提交配置。

图1-15 配置 IP-MAC 绑定

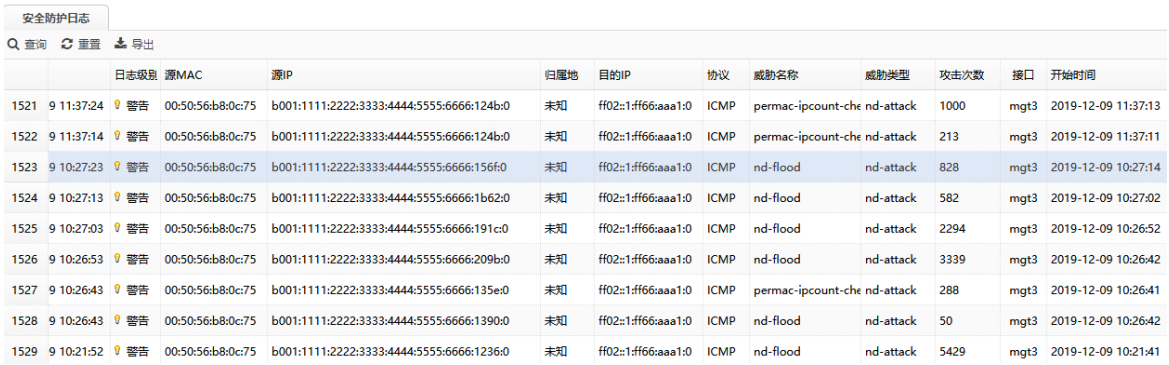
进入“策略配置 > 安全设置 > 安全防护 > ARP/ND 攻击防护 > ARP/ND Flood 攻击”；设置阈值和抑制时长，然后点击提交按钮提交配置。

图1-16 配置 ND Flood 攻击防护

3. 验证配置

如下图所示，进入“数据中心>安全日志>安全防护日志”，进入安全防护日志显示页面，可以查看防 ND 欺骗日志。

图1-17 安全防护日志



		日志级别	源MAC	源IP	归属地	目的IP	协议	威胁名称	威胁类型	攻击次数	接口	开始时间
1521	9 11:37:24	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:124b:0	未知	ff02::1:ff66:aaa1:0	ICMP	permac-ipcount-che	nd-attack	1000	mgt3	2019-12-09 11:37:13
1522	9 11:37:14	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:124b:0	未知	ff02::1:ff66:aaa1:0	ICMP	permac-ipcount-che	nd-attack	213	mgt3	2019-12-09 11:37:11
1523	9 10:27:23	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:156f:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	828	mgt3	2019-12-09 10:27:14
1524	9 10:27:13	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:1b62:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	582	mgt3	2019-12-09 10:27:02
1525	9 10:27:03	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:191c:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	2294	mgt3	2019-12-09 10:26:52
1526	9 10:26:53	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:209b:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	3339	mgt3	2019-12-09 10:26:42
1527	9 10:26:43	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:135e:0	未知	ff02::1:ff66:aaa1:0	ICMP	permac-ipcount-che	nd-attack	288	mgt3	2019-12-09 10:26:41
1528	9 10:26:43	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:1390:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	50	mgt3	2019-12-09 10:26:42
1529	9 10:21:52	警告	00:50:56:b8:0c:75	b001:1111:2222:3333:4444:5555:6666:1236:0	未知	ff02::1:ff66:aaa1:0	ICMP	nd-flood	nd-attack	5429	mgt3	2019-12-09 10:21:41

1.2 异常报文攻击防护

1.2.1 异常报文攻击防护概述

在网络中，有时会有一些带有攻击性质的报文传输，通常这些报文能对目标主机进行破坏，异常报文攻击防护能对这些报文进行拦截并报日志。

1.2.2 异常报文攻击防护配置

通过菜单“策略配置 > 安全设置 > 安全防护 > 异常包攻击防御”进入异常包攻击防御的配置界面，如图 1-18 所示。

图1-18 异常报文攻击防护设置界面

表1-7 异常报文攻击防护详细配置描述表

配置项	说明
Ping of Death	ping-of-death攻击是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，丢弃攻击报文并根据配置输出告警日志信息。
Land-Base	Land-base攻击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Lland-base攻击，丢弃攻击报文并根据配置输出告警日志信息。
Tear-drop	tear-drop攻击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，并输出告警日志信息。 因为正常报文传送也有可能出现报文重叠，因此设备不会丢弃该报文，而是采取裁减、重新组装报文的方式，发送出正常的报文。
Tcp flag	TCP 异常攻击防护功能开启后，缺省情况下当安全网关发现受到TCP 异常攻击后，会丢弃攻击包。

配置项	说明
Winnuke	Winnuke攻击通过向目的主机的139、138、137、113、53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，可以检测出Winnuke攻击报文，丢弃攻击报文并根据配置输出告警日志信息。
Smurf	这种攻击方法结合使用了IP欺骗和ICMP回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务。 Smurf攻击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。
IP-Spoof	防护IP地址欺骗攻击，暂时用反向路由检测来实现，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。
Jolt2	Jolt2攻击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。
tcp sack	当tcp 的mss很小，并且不停发布连续报文时，会触发漏洞。

1.2.3 异常报文攻击防护配置举例

1. 用户需求

配置异常报文攻击防护，开启 Land-Base 攻击防护和 IP-Spoof 攻击防护。

2. 配置步骤

通过菜单“策略配置 > 安全设置 > 安全防护 > 异常包攻击防御”打开异常报文攻击防御显示页面，点击勾选 Land-Base 攻击防护和 IP-Spoof 攻击防护选项，如图 1-19 所示，点击<提交>按钮，配置完成。

图1-19 异常包攻击防御配置页面

1.3 IPv6异常报文防护

1.3.1 IPv6 异常报文防护配置

如图 1-20 所示，通过菜单“策略配置>安全设置>安全防护>异常包攻击防御>IPv6 异常包攻击”使用该功能。

图1-20 IPv6 异常包攻击防御的配置界面

表1-8 IPv6 异常包攻击详细信息描述表

配置项	说明
Winnuke	winnuke报文攻击
Land-Base	Land-Base报文攻击
TCP flag	异常的TCP flag报文攻击
Fraggle	Fraggle报文攻击
IP Spoof	IP地址欺骗攻击

说明

IPv6 异常包攻击的配置和显示等都在一个页面。

1.3.2 IPv6 异常包攻击防护举例

1. 用户需求

配置设备 进行 IPv6 异常的 TCP flag 报文攻击防护功能。

2. 配置步骤

如图 1-21 所示，通过菜单“策略配置 > 安全设置 > 安全防护 > 异常包攻击防御 > IPv6 异常包攻击”打开显示页面，点击勾选 TCP flag 攻击防护选项，点击<提交>按钮，配置完成。

图1-21 IPv6 异常包攻击配置页面

1.4 扫描攻击防护

1.4.1 扫描攻击防护概述

扫描攻击是指，攻击者运用扫描工具对网络进行主机地址或端口的扫描，通过准确定位潜在目标的位置，探测目标系统的网络拓扑结构和启用的服务类型，为进一步侵入目标系统做准备。设备可以有效防范以上攻击，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。

1.4.2 扫描攻击防护配置

通过菜单“策略配置 > 安全设置 > 安全防护 > 异常包攻击防御 > 扫描攻击防御”进入扫描攻击防御显示界面，如图 1-22 所示。点击<新建>按钮，进入新建扫描攻击防御界面，如图 1-23 所示。

图1-22 扫描攻击防御显示界面

说明

在该页面上，显示所有配置的扫描攻击防护表项，同时能够<新建>、<编辑>和<删除>等。

图1-23 扫描攻击防御新建页面

表1-9 扫描攻击防御详细信息描述表

配置项	说明
选择接口	选择需要防护的接口
扫描阈频率	需要防护的阈值
加入黑名单	启用加入黑名单的选项
加入黑名单的时间	将源IP加入黑名单的时间

1.4.3 扫描攻击防护配置举例

1. 用户需求

开启 ge1 接口的扫描攻击防御功能，采用缺省配置。

2. 配置步骤

(1) 如图 1-24 所示，通过菜单“策略配置 > 安全设置 > 安全防护 > 异常包攻击防御 > 扫描攻击防御”打开显示页面，点击显示页面的<新建>按钮。

图1-24 扫描攻击防御显示界面

(2) 如图 1-25 所示，在弹出的新建页面中进行配置，勾选“启用端口扫描防护”和“启用 IP 扫描防护”，使用缺省配置。

图1-25 扫描攻击防御配置界面

(3) 点击<提交>按钮，完成扫描攻击防护的配置。

3. 验证配置

如图 1-26 所示，通过菜单“策略配置 > 安全设置 > 安全防护 > 异常包攻击防御 > 扫描攻击防御”打开扫描攻击防御显示页面，在显示页面中看到刚才配置的规则，如图 1-26 所示。

图1-26 扫描攻击防御配置结果

1.5 DoS攻击防护

1.5.1 DoS 攻击防护概述

DoS 攻击是指，攻击者在短时间内向目标系统发送大量的虚假请求，导致目标系统疲于应付无用信息，而无法为合法用户提供正常服务，即发生拒绝服务。

当前支持对以下四种攻击进行有效防范：

1. 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。

2. 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。

3. 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。

4. DNS Flood 攻击

DNS Query Flood 攻击采用的方法是向被攻击的 DNS 服务器发送大量的域名解析请求，通常请求解析的域名是随机生成或者是网络上根本不存在的域名。被攻击的 DNS 服务器在接收到域名解析请求时，首先会在服务器上查找是否有对应的缓存，如果查找不到并且该域名无法直接由服务器解析时，DNS 服务器会向其上层 DNS 服务器递归查询域名信息。域名解析的过程给服务器带来了很大的负载，每秒钟域名解析请求超过一定的数量就会造成 DNS 服务器解析域名超时。

1.5.2 目的 IP 防御设置

通过菜单“策略配置 > 安全设置 > 安全防护 > DoS 攻击防护 > 目的 IP 防御”进入目的 IP 防御的显示界面，如图 1-27 所示。点击<新建>按钮，弹出目的 IP 防御的配置界面，如图 1-28 所示。

图1-27 目的 IP 防御显示界面

图1-28 新建目的 IP 防御界面

表1-10 配置说明

配置项	说明
指定保护主机的IP地址	指定保护地址范围
SYN Flood阈值	每秒发往目的IP的最大SYN报文个数
UDP Flood阈值	每秒发往目的IP的最大UDP报文个数
ICMP Flood阈值	每秒发往目的IP的最大ICMP报文个数
DNS Flood阈值	每秒发往目的IP的最大DNS报文个数

1.5.3 目的 IP 防御配置举例

1. 用户需求

配置保护 IP 地址为 1.1.1.1-1.1.1.10，开启 UDP Flood 防御阈值为 1000 的规则。

2. 配置步骤

(1) 如图 1-29 所示，通过菜单“策略配置>安全设置>安全防护>DoS 攻击防护>目的 IP 防御”打开显示页面，点击上面的<新建>按钮，如图 1-30 所示，在弹出的新建页面中进行配置。

图1-29 目的 IP 防御显示页面

图1-30 目的 IP 防御配置页面

(2) 完成配置后，点击<提交>按钮，规则创建成功。

1.5.4 接口防御设置

通过菜单“策略配置 > 安全设置 > 安全防护 > DoS 攻击防护 > 接口防御”进入接口防御显示界面，如图 1-31 所示。点击<新建>按钮后，将弹出新建接口防御界面，如图 1-32 所示。

图1-31 接口防御显示界面

图1-32 接口防御新建页面

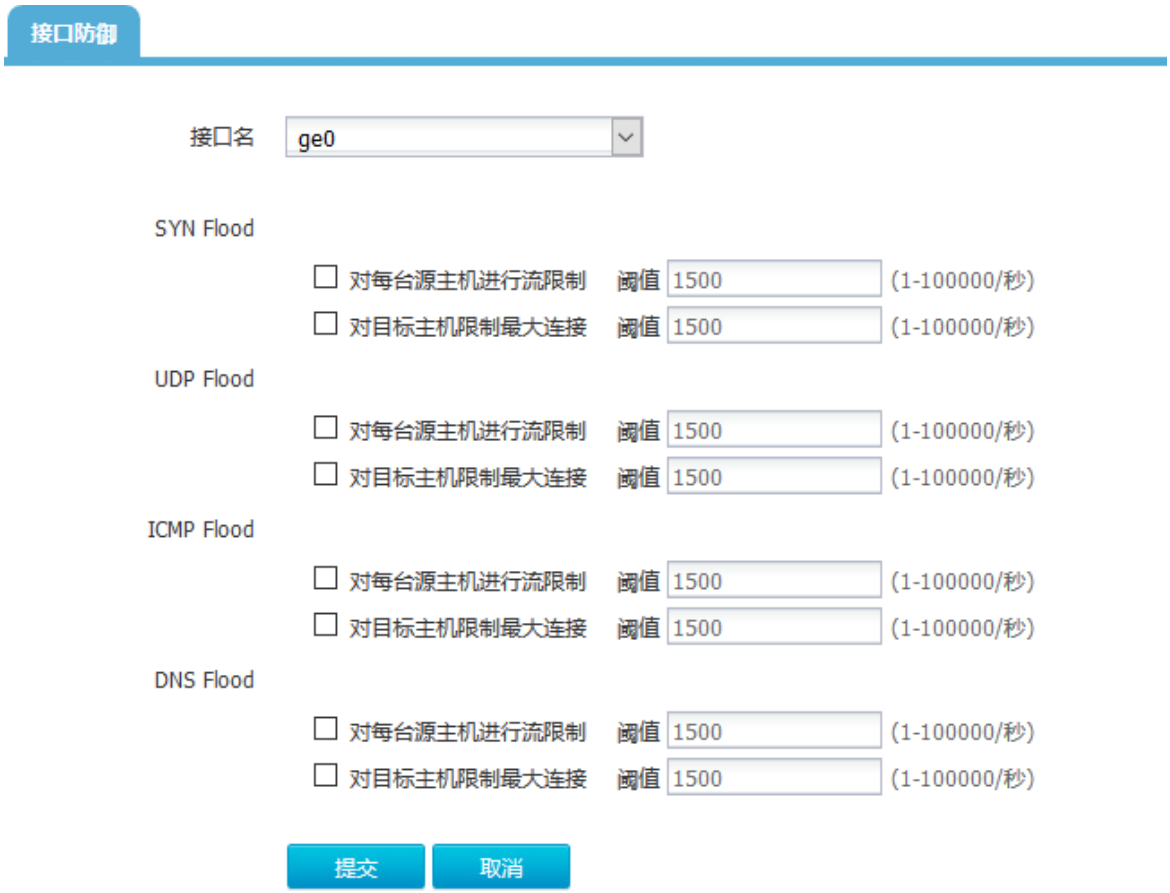


表1-11 配置说明

配置项	说明
接口名	选择需要防护的接口名称
SYN Flood选项	对每台源主机进行流限制：设置源主机的流限制阈值 对目标主机限制最大连接：设置目的主机的最大连接
UDP Flood选项	对每台源主机进行流限制：设置源主机的流限制阈值 对目标主机限制最大连接：设置目的主机的最大连接
ICMP Flood选项	对每台源主机进行流限制：设置源主机的流限制阈值 对目标主机限制最大连接：设置目的主机的最大连接
DNS Flood选项	对每台源主机进行流限制：设置源主机的流限制阈值 对目标主机限制最大连接：设置目的主机的最大连接

1.5.5 接口防御配置举例

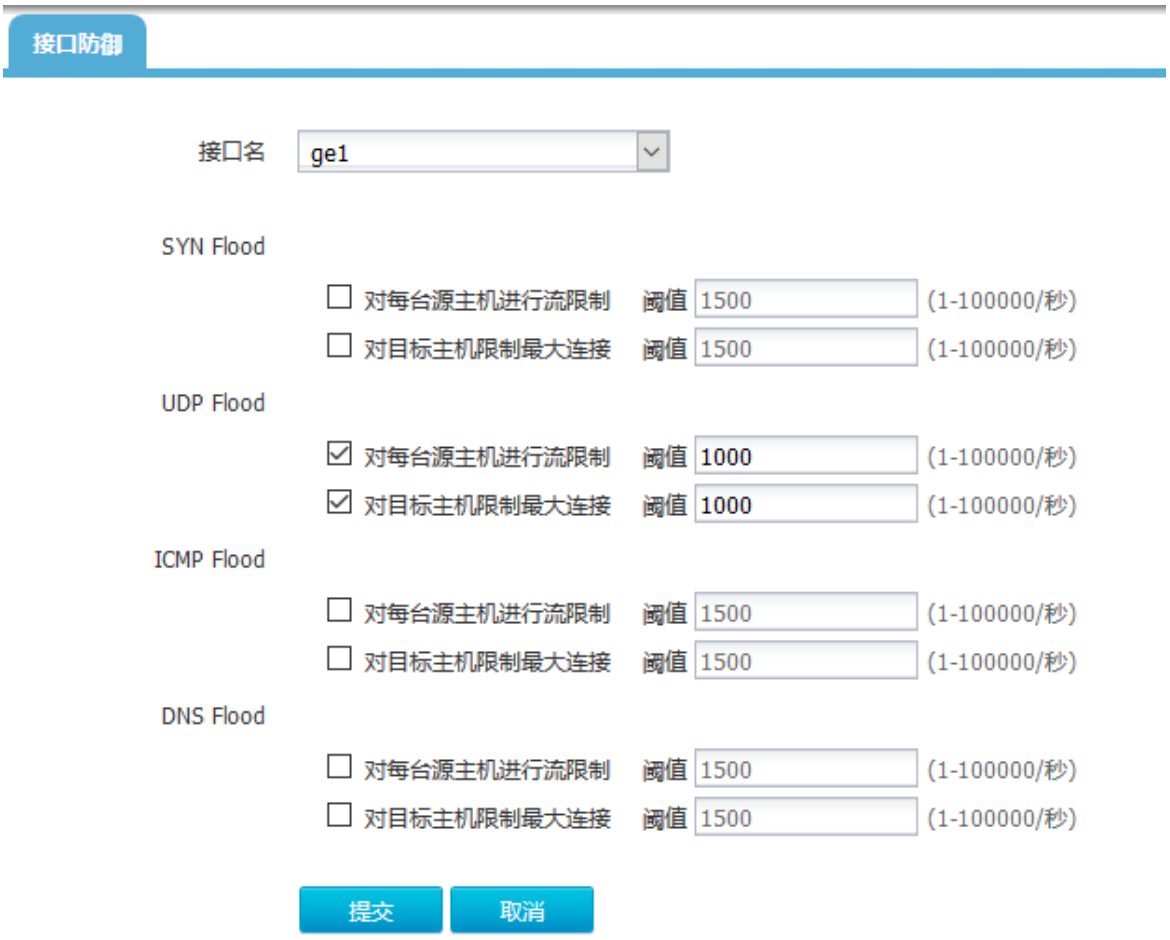
1. 用户需求

ge1 接口，开启 UDP flood 防御，并设置其对源主机和目的主机的限制阈值都为 1000。

2. 配置步骤

通过菜单“策略配置 > 安全设置 > 安全防护 > DoS 攻击防护 > 接口防御”，打开如图 1-33 所示接口防御的显示页面，点击<新建>按钮，在弹出的新建页面进行配置。配置完成后，点击<提交>按钮，完成接口防御的配置。

图1-33 接口防御配置页面



1.6 IPMAC绑定

1.6.1 IPMAC 概述

Address Resolution Protocol (ARP)是寻找 IP 地址所对应的 MAC 地址的一种协议。

在以太网中，对于处于同一子网的两个通信实体来说，一次 IP 通信过程大致如下：

当源端发送一个 IP 包之前，它必须知道目的端的 MAC 地址才可以完成封装，可是此时源端只能知道目的端的 IP 地址（通过用户的事先配置或者查路由表），这样就必须依靠 ARP 协议来完成目的端 MAC 地址的解析。因此源端发送一个包含目的 IP 地址的 ARP 请求，目的端收到后向源端返回 ARP 应答，通告自己的 MAC 地址，源端获得目的端 MAC 地址后才可以将 IP 包封装在以太网头中发送出去。

由于网络中可能存在一些攻击软件仿冒某台主机上网，逃过跟踪。为了避免这种情况，设备实现了 IP-MAC 绑定功能，把用户的 MAC 和 IP 绑定起来。配置了 IP-MAC 绑定后，通过设备的报文的 MAC 和 IP 必须严格一致，否则报文将被丢弃。

1.6.2 IPMAC 绑定添加

通过菜单“策略配置>安全设置>安全防护>ARP 攻击防护>IP-MAC 绑定”进入 IP-MAC 绑定显示界面，如图 1-34 所示。点击<新建>按钮后，将弹出新建 IP-MAC 绑定界面，如图 1-35 所示。

图1-34 IPMAC 绑定显示界面

图1-35 IP-MAC 绑定添加

表1-12 配置说明

配置项	说明
名称	IP-MAC绑定项的名称
描述	规则描述信息

配置项	说明
IP地址	绑定的IP地址
MAC地址	绑定的MAC地址
唯一性	绑定类型 开启表示一个MAC和一个IP地址唯一对应，关闭表示一个MAC地址和多个IP地址对应

1.6.3 IPMAC 绑定配置举例

1. 用户需求

配置名为 test 的 IPMAC 绑定规则，将 IP 地址 2.2.2.2 和 MAC 地址 00:de:ad:00:00:0c 进行绑定。

2. 配置步骤

(1) 通过菜单“策略配置>安全设置>安全防护>ARP 攻击防护>IP-MAC 绑定”打开如图 1-36 的 IPMAC 绑定显示页面，点击<新建>按钮。

(2) 在弹出的新建页面中，对规则进行配置，完成后点击<提交>按钮。

图1-36 IPMAC 绑定配置页面

1.7 防ARP攻击

1.7.1 防 ARP 攻击概述

在局域网中，通信前必须通过 ARP 协议将 IP 地址转换为 MAC 地址。ARP 协议对网络安全具有重要的意义，但是当初 ARP 方式的设计没有考虑到过多的安全问题，留下很多隐患，使得 ARP 攻击成为当前网络环境中遇到的一个非常典型的安全威胁。

通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量，使网络阻塞，攻击者只要持续不断的发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存，造成网络中断或中间人攻击。

受到 ARP 攻击后会出现无法正常上网、ARP 包爆增、不正常或错误的 MAC 地址、一个 MAC 地址对应多个 IP、IP 冲突等情况。ARP 攻击因为技术门槛低，易于实现，在现今的网络中频频出现，有效防范 ARP 攻击已成为确保网络畅通的必要条件。

设备的防 ARP 攻击功能有效识别 ARP 欺骗攻击和 ARP flood 攻击，对疑似攻击的行为告警，并配合 IP-MAC 绑定、主动保护发包及关闭 ARP 学习等，有效防范 ARP 攻击造成的损害。

1.7.2 ARP 表项显示

通过菜单“策略配置 > 安全设置 > 安全防护 > ARP 攻击防护 > ARP 表”进入 ARP 表显示界面，如图 1-37 所示。

图1-37 ARP 表项显示

1.7.3 ARP Flood 攻击防护

如图 1-38 所示，通过菜单“策略配置 > 安全设置 > 安全防护 > ARP 攻击防护 > ARP Flood 攻击”使用该功能。

图1-38 ARP Flood 攻击设置页面

表1-13 ARP Flood 攻击防护详细配置描述表

配置项	说明
启用	点选启用防ARP Flood攻击
ARP攻击识别阈值	一秒内收到ARP报文的数量，缺省配置为300个/秒
攻击主机抑制时长	设置阻断时间，当系统检测到攻击时，在配置的时长内拒绝来自于该台源主机的所有其它包，缺省配置为60秒

1.7.4 防 ARP 欺骗

如图 1-39 所示，通过菜单“策略配置 > 安全设置 > 安全防护 > ARP 攻击防护 > 防 ARP 欺骗”使用该功能。

图1-39 防 ARP 欺骗设置页面

表1-14 防 ARP 欺骗详细信息描述表

配置项	说明
ARP防欺骗攻击	点选启用ARP防欺骗攻击
关闭ARP学习	缺省情况下启用ARP学习，关闭后只要是不匹配IP-MAC绑定表的报文都将被丢弃
主动保护	点选启用主动保护发包功能，每隔一定时间间隔发送一次主动保护列表上的免费ARP报文
时间间隔	发送主动保护列表上的ARP的时间间隔，缺省配置为1秒

1.7.5 主动保护列表添加

点选图 1-40 防 ARP 欺骗设置页面中的保护列表下的<新建>按钮后，将弹出如下页面。

图1-40 主动保护列表页面

表1-15 主动保护详细信息描述表

配置项	说明
接口	ARP报文发送接口
接口保护	在保护列表中加入接口地址
IP地址&MAC地址	广播ARP报文的IP和MAC

1.7.6 主动保护列表配置举例

1. 用户需求

将接口 ge1 加入防 ARP 欺骗的主动保护列表中。保护的 IP 和 MAC 分别为：2.2.2.2 和 00:de:ad:00:00:0c。

2. 配置步骤

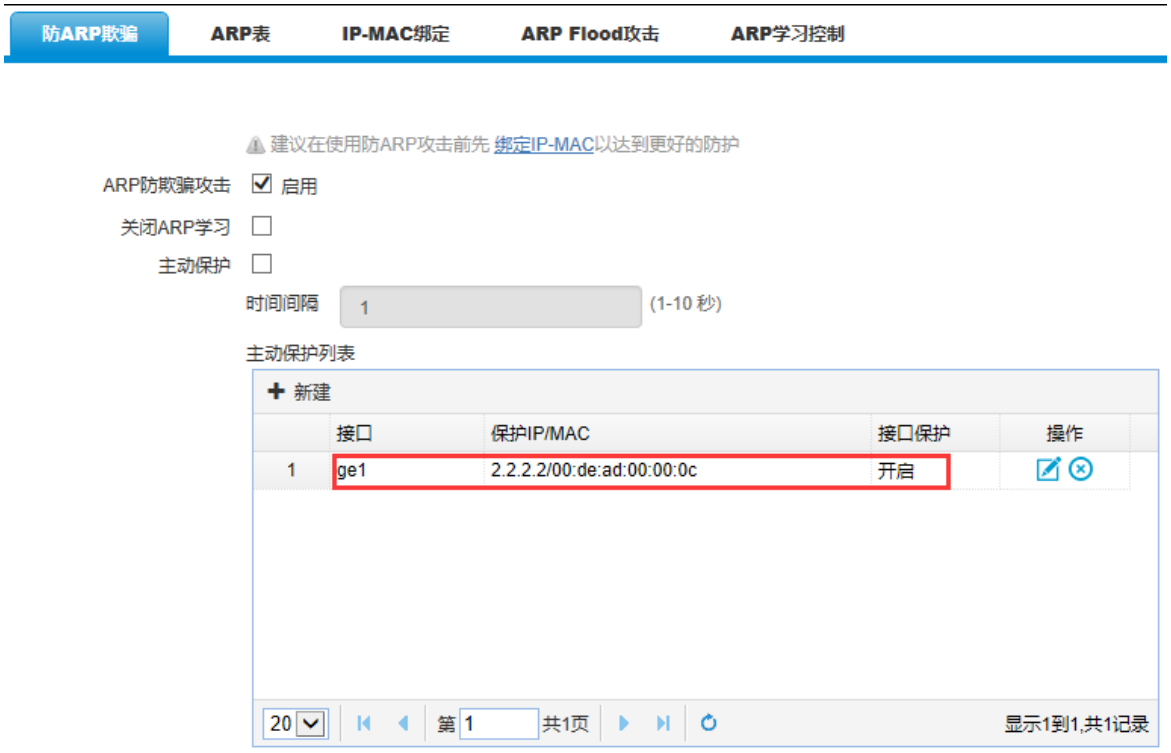
(1) 先选中图 1-41 防 ARP 欺骗设置中的 ARP 防欺骗攻击<启用>按钮，可以看到主动保护列表下的<新建>按钮可选了，点击后会弹出主动保护列表的配置页面。

(2) 选择接口为 ge1，输入要保护的 IP 和 MAC 地址，点击“添加到列表”。

图1-41 主动保护列表配置页面

(3) 如图 1-42 所示，点击<提交>按钮后，可以在防 ARP 欺骗页面看到我们加入的 ge1 接口。

图1-42 防 ARP 欺骗页面



1.8 行为模型

1.8.1 行为模型简介

行为模型（又名 DNS 隧道），是隐蔽信道的一种，通过将其它协议封装在 DNS 协议中传输建立通信。因为在我们的网络世界中 DNS 是一个必不可少的服务，所以大部分防火墙和入侵检测设备很少会过滤 DNS 流量，这就给 DNS 作为一种隐蔽信道提供了条件，从而可以利用它实现诸如远程控制，文件传输等操作，现在越来越多的研究证明 DNS 隧道也经常在僵尸网络和 APT 攻击中扮演者重要的角色，因此 DNS 隐蔽隧道检测势在必行。

设备通过对 DNS 隐蔽隧道特征的提取和特征综合分析，来实现对 DNS 隐蔽隧道的检测，从而阻止 DNS 隧道带来的威胁。

1.8.2 行为模型配置页面

通过菜单“策略配置>安全设置>安全防护>行为模型”，编辑 DNS 隧道检测，点击<编辑>，进入如图 1-43 所示页面。各个配置项含义如表 1-16 所示。

图1-43 DNS 隧道配置页面

表1-16 DNS 隧道配置各项含义表

标题项	说明
开启	是否开启dns隧道功能
日志	记录dns隧道日志（在安全日志-行为模型日志）
检测宽松度	严格、适中、宽松，默认适中。严格的阈值为50，适中的阈值为100，宽松的阈值为200
检测方式	所有、基于异常报文、基于流量模型
处理动作	允许或拒绝
使用预置白名单	设备配置的DNS服务器地址，默认勾选（开启后不会在走dns-tunnel流程）dns透明代理和dns缓存不算在里面
添加自定义白名单	64个

1.8.3 行为模型配置举例

1. 组网需求

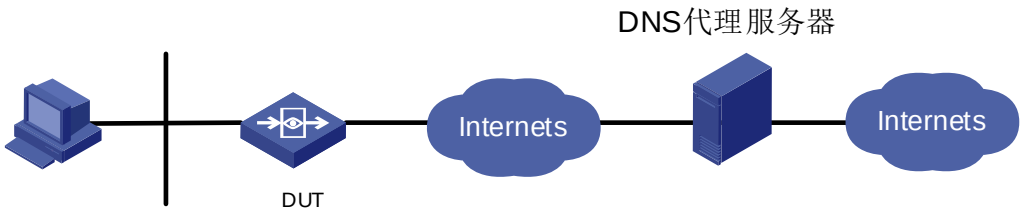
针对公司内部网络，设备需要开启DNS检测功能避免内网用户被远程黑客控制成为僵尸网络和APT攻击，公司出口开启了 DNS 服务功能，先检测分析日志。

(1) 在 DNS 隧道模块里直接启用使用预置白名单；

(2) 自定义白名单加入了运营商提供的 DNS 服务器。

2. 组网图

图1-44 行为模型组网图



3. 配置步骤

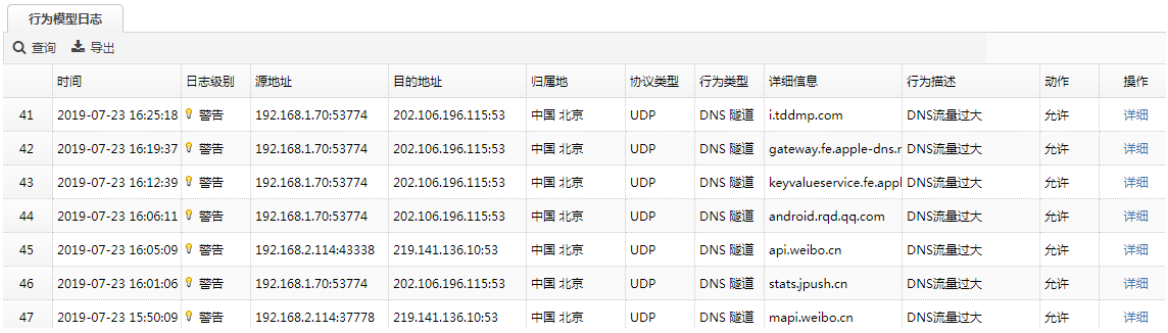
(1) 启用 DNS 隧道，在导航栏中选择“策略配置>安全设置>安全防护>行为模型”，编辑 DNS 隧道检测，点击<编辑>启用 DNS 隧道检测记录日志，处理动作为允许，如图 1-45 所示。

图1-45 编辑 DNS 隧道检测

(2) 点击<提交>按钮，提交配置。

在导航栏中选择“数据中心>日志中心>安全日志>行为模型日志”。查看分析行为模型日志，如图1-46 所示。

图1-46 行为模型日志



	时间	日志级别	源地址	目的地址	归属地	协议类型	行为类型	详细信息	行为描述	动作	操作
41	2019-07-23 16:25:18	警告	192.168.1.70:53774	202.106.196.115:53	中国 北京	UDP	DNS 隧道	i.tddmp.com	DNS流量过大	允许	详细
42	2019-07-23 16:19:37	警告	192.168.1.70:53774	202.106.196.115:53	中国 北京	UDP	DNS 隧道	gateway.fe.apple-dns.r	DNS流量过大	允许	详细
43	2019-07-23 16:12:39	警告	192.168.1.70:53774	202.106.196.115:53	中国 北京	UDP	DNS 隧道	keyvalueservice.fe.appl	DNS流量过大	允许	详细
44	2019-07-23 16:06:11	警告	192.168.1.70:53774	202.106.196.115:53	中国 北京	UDP	DNS 隧道	android.rqd.qq.com	DNS流量过大	允许	详细
45	2019-07-23 16:05:09	警告	192.168.2.114:43338	219.141.136.10:53	中国 北京	UDP	DNS 隧道	api.weibo.cn	DNS流量过大	允许	详细
46	2019-07-23 16:01:06	警告	192.168.1.70:53774	202.106.196.115:53	中国 北京	UDP	DNS 隧道	stats.jpush.cn	DNS流量过大	允许	详细
47	2019-07-23 15:50:09	警告	192.168.2.114:37778	219.141.136.10:53	中国 北京	UDP	DNS 隧道	mapi.weibo.cn	DNS流量过大	允许	详细

(3) 启用 DNS 隧道，在导航栏中选择“策略配置>安全设置>安全防护>行为模型”，编辑 DNS 隧道检测，点击<编辑>启用 DNS 隧道检测记录日志，处理动作为拒绝并加入黑名单 1 小时，如图 1-47 所示。

图1-47 编辑 DNS 隧道检测

(4) 点击<提交>按钮，提交配置。

4. 验证配置

在导航栏中选择“数据中心>日志中心>安全日志>行为模型日志”。查看，如图 1-48 所示。

图1-48 行为模型日志

在导航栏中选择“数据中心>系统监控>黑名单记录”。查看黑名单记录，被检测出来的 DNS 服务器地址加入黑名单，如图 1-49 所示。

图1-49 黑名单

1.9 防暴力破解

1.9.1 防暴力破解简介

暴力破解是指攻击者通过穷举的方法登录相应服务从而获得可以登录的用户名密码对。通过检测出流量中的暴力破解行为并进行阻断。用户可配置是否开启暴力破解防御，服务类型，支持的服务类型包括 ftp、telnet、smtp、http、imap、mssql、mysql、oracle、pop3、postgres，各个服务单独配置暴力破解检测时长和阈值，配置是否把攻击者加入黑名单。

1.9.2 防暴力破解配置

如图 1-50 所示，在导航栏中选择“策略配置>安全设置>安全防护>防暴力破解”，进入防暴力破解的配置界面。

图1-50 防暴力破解配置界面

表1-17 防暴力破解界面详细描述表

标题项	说明
启用	勾选启用/禁用防暴力破解功能
服务	选择监测的服务
Web登录保护	勾选启用/禁用web登录保护功能
url路径	Web登录保护的url
攻击者加入黑名单	勾选启用/禁用攻击者加入黑名单功能

1.9.3 服务选择

如图 1-51 所示，在导航栏中选择“策略配置>安全设置>安全防护>防暴力破解”，点击“请选择服务”弹出服务的配置界面。

图1-51 服务配置界面

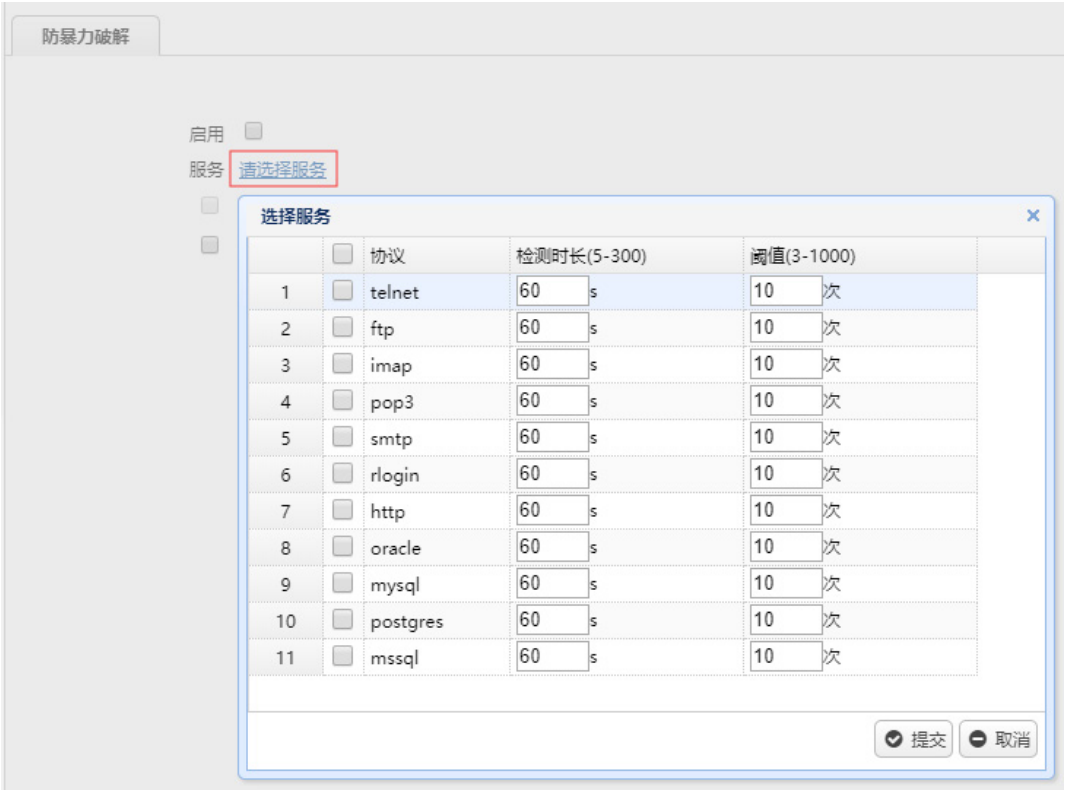


表1-18 服务配置界面详细描述表

标题项	说明
协议	勾选需要开启防暴力破解功能的服务
检测时长	防暴力破解的检测周期
阈值	攻击次数，达到阈值触发防暴力破解记录攻击事件

1.10 弱密码防护

1.10.1 弱密码防护简介

对于密码明文传输的服务，从登录报文中提取出密码并判断出密码强度，若为弱密码则产生日志但不阻断登录。支持的服务包括 ftp、imap、pop3、smtp、telnet。用户可以配置开启或者关闭弱密码检测功能，目标服务，弱密码密码强度。

1.10.2 弱密码防护

如图 1-50 所示，在导航栏中选择“策略配置>安全设置>安全防护>弱密码防护”，进入弱密码防护的配置界面。

图1-52 弱密码防护配置界面

表1-19 防暴力破解界面详细描述表

标题项	说明
启用	勾选启用/禁用弱密码防护功能
服务	选择检测的服务
弱密码规则	勾选启用/禁用弱密码防护规则
自定义密码	配置自定义弱密码字典

1.10.3 服务选择

如图 1-51 所示，在导航栏中选择“策略配置>安全设置>安全防护>弱密码防护”，点击“选择服务”弹出服务配置页面。

图1-53 服务配置界面

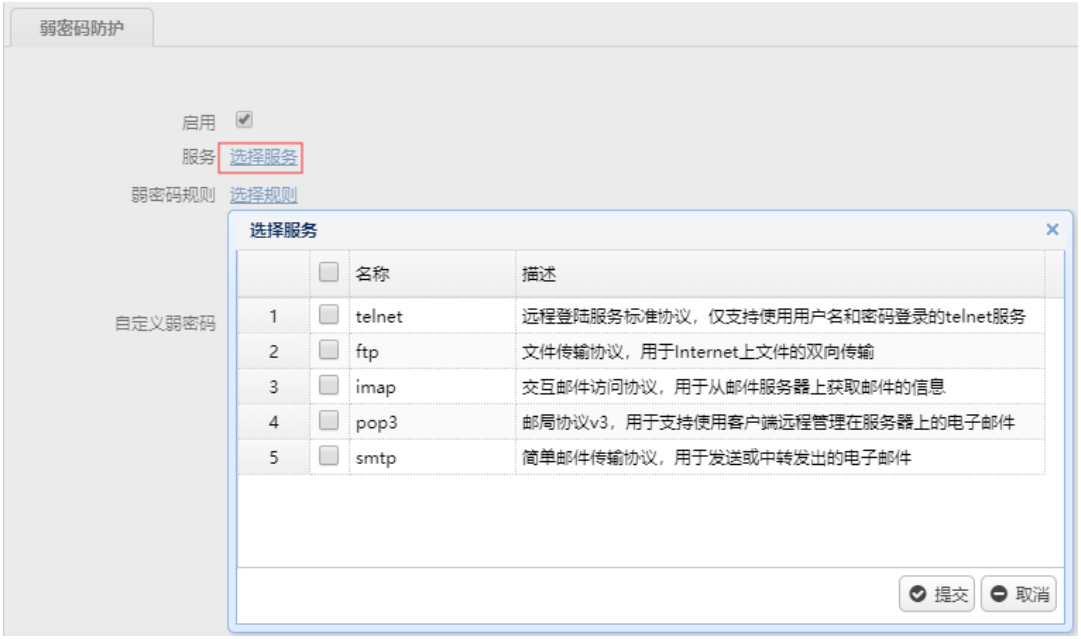


表1-20 服务配置界面详细描述表

标题项	说明
名称	服务名称
描述	服务的功能描述

1.10.4 弱密码规则

如图 1-54 所示，在导航栏中选择“策略配置>安全设置>安全防护>弱密码防护”，点击“选择规则”弹出弱密码规则配置页面。

图1-54 规则配置界面

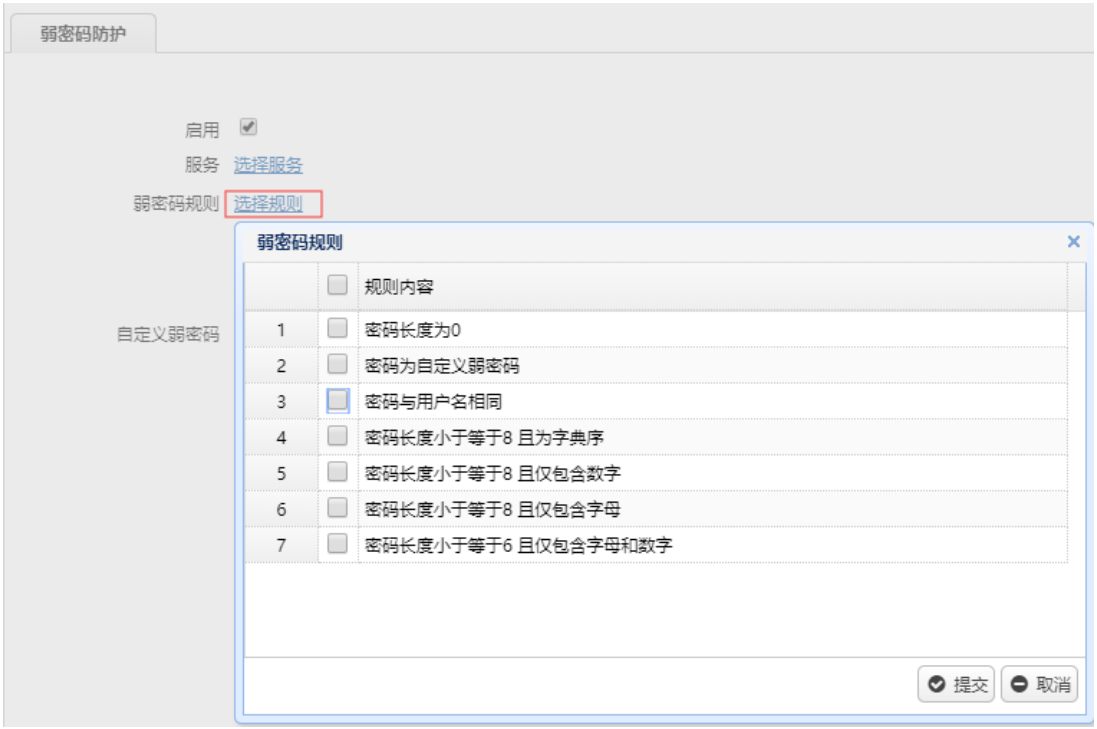


表1-21 规则配置界面详细描述表

标题项	说明
规则内容	勾选规则的详细描述

1.11 非法外联防护

1.11.1 非法外联防护简介

为保证内部网络的安全可靠运行，通常采用以下两种方式对内外网实施安全隔离：

(1) 内、外网物理隔离

内、外网进行物理隔离，严格上来讲，内外网根本就没有连通，不能相互通信，专职人员必须使用物理隔离的计算机才能访问内外网。

(2) 内、外网逻辑隔离

内、外网逻辑隔离，主要是通过划分 VLAN 等技术手段，隔离一些特殊群体，以实施更有针对性的安全防护，实现内部网络的相对独立性。同时在内外网连接处，一般安装防火墙或入侵检测系统对内网提供保护。

但是，非法外联和非法接入等行为，很容易对物理隔离和逻辑隔离的内部网络造成损害。

针对以上情况通过对内部网络终端或者服务器的外联行为进行识别，设定允许终端或者服务器外联的地址、外联地址的服务及端口来定义正常外联行为，定义的正常外联行为之外的所有外联行为全部作为非法外联。

1.11.2 非法外联防护

1. 非法外联防护策略

如图 1-50 所示，在导航栏中选择“策略配置>安全设置>安全防护>非法外联防护”，进入非法外联防护策略的配置界面。

图1-55 非法外联防护策略配置界面

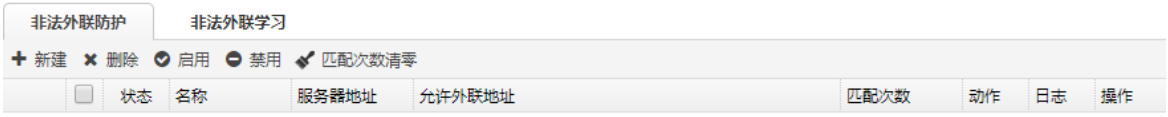


表1-22 非法外联防护界面详细描述表

标题项	说明
新建	新建策略
删除	删除勾选的策略
启用	启用勾选的策略
禁用	禁用勾选的策略
匹配次数清零	清空勾选的策略
操作-编辑	编辑该条策略
操作-删除	删除该条策略

2. 新建策略

如图 1-51 所示，在导航栏中选择“策略配置>安全设置>安全防护>非法外联防护”，进入非法外联防护策略的配置界面。点击“新建”创建策略。

图1-56 策略配置界面

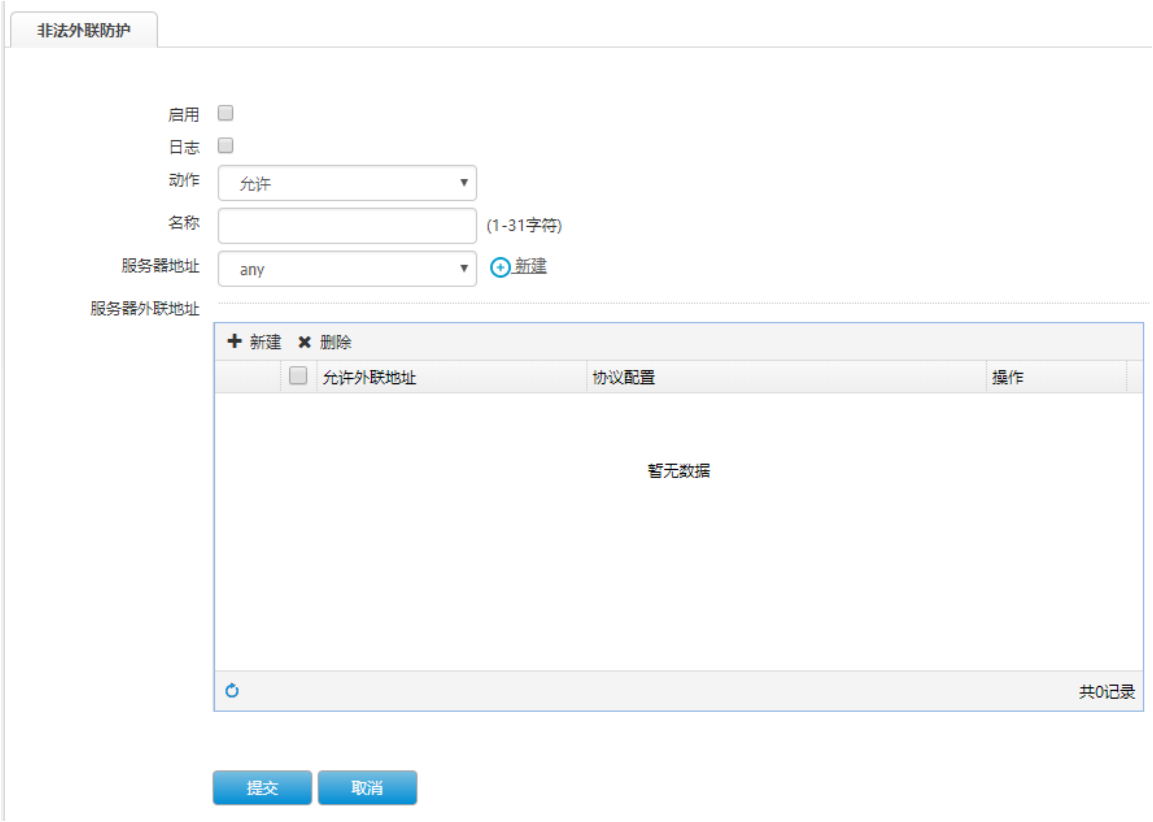


表1-23 字典配置界面详细描述表

标题项	说明
启用	勾选启用策略
日志	勾选开启日志记录
动作	匹配策略的数据允许/拒绝通过
服务器地址	保护的内网服务器地址
服务器外联地址	内网允许访问的外网地址

3. 新建服务器外联地址

如图 1-57 所示，在导航栏中选择“策略配置>安全设置>安全防护>非法外联防护”，点击“新建”进入非法外联防护策略的配置界面，在“服务器外联地址”中，点击“新建”弹出服务器外联地址的配置窗口。

图1-57 服务器外联地址配置界面

表1-24 字典配置界面详细描述表

标题项	说明
允许外联地址	允许外联地址，支持ip和域名配置。
Tcp	允许外联的tcp端口，最多支持128个端口。
Udp	允许外联的udp端口，最多支持128个端口。
ICMP	勾选是否允许ping包。

1.11.3 非法外联学习

如图 1-58 所示，在导航栏中选择“策略配置>安全设置>安全防护>非法外联防护>非法外联学习”，进入非法外联学习的配置界面。

图1-58 非法外联学习配置界面

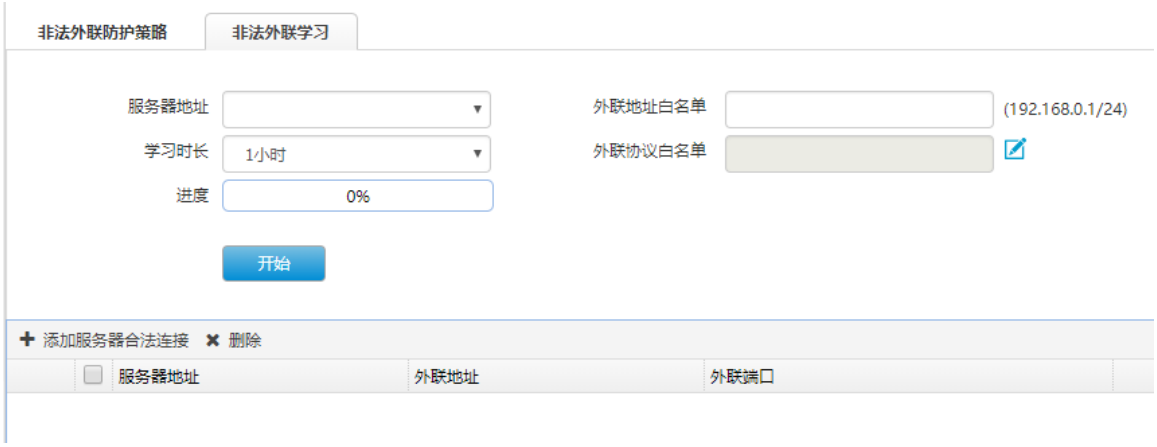


表1-25 非法外联学习界面详细描述表

标题项	说明
服务器地址	学习的服务器地址
学习时长	选择学习时长
进度	显示学习进度
外联地址白名单	不参与学习的外联目的地址
外联协议白名单	不参与学习的外联目的端口
开始	开始学习
添加服务器合法连接	学习到的外联地址添加到防护中服务器外联地址

目 录

1 WEB 安全防护 ····· 1-1
1.1 WEB 安全防护简介 ····· 1-1
1.2 防护策略 ····· 1-1
1.2.1 防护策略配置 ····· 1-1
1.2.2 精确访问控制 ····· 1-3
1.2.3 规则防护 ····· 1-4
1.2.4 防盗链 ····· 1-6
1.2.5 CSRF 攻击防护 ····· 1-7
1.2.6 CC 攻击防护 ····· 1-9
1.2.7 网页防篡改 ····· 1-9
1.2.8 应用隐藏 ····· 1-10
1.3 规则库 ····· 1-11
1.4 防篡改网页缓存 ····· 1-12

1 WEB 安全防护

1.1 WEB安全防护简介

随着网络信息化的发展，越来越多的企业利用 WEB 应用系统提供客户服务，进行产品推广、市场宣传、培训服务、远程服务协作甚至网上交易。WEB2.0 的发展更是加强了用户和 WEB 服务之间的交互性，但是各种安全问题也随之而来。WEB 应用数据被窃取、网页被篡改，甚至 WEB 站点成为传播木马的傀儡，给更多访问者造成危害，带来损失；也对政府、公司形象造成严重的破坏。

WEB 防护功能通过增加 WEB 应用防护策略，匹配条件是源地址、目的地址（Web 服务器地址）和端口，同时在策略下配置各个防护功能（规则防护、精确访问控制、防盗链、CSRF 攻击防护、CC 攻击防护、应用隐藏、网页防篡改），当报文匹配策略时，就会逐一进行防护功能的处理，并执行相应的动作。可以帮助用户进行 Web 安全防御，提高网站安全性，而且集成了网络爬虫识别和过滤、网站资源盗链防护、内容关键字过滤、HTTP 协议合规性和 URL 参数合规性检查等功能，帮助用户对网站的访问进行过滤和优化，提高网站运营的稳定性和服务质量。

1.2 防护策略

1.2.1 防护策略配置

如图 1-1 所示，在导航栏中选择“策略配置>安全设置>WEB 防护>防护策略”，进入防护策略界面。

图1-1 防护策略界面

表1-1 防护策略界面详细描述表

标题项	说明
名称	策略名称
源地址	策略匹配的源地址
目的地址	策略匹配的目的地址
服务端口	HTTP服务的端口默认80
描述	策略描述
启用	策略状态
防护配置	策略启用的防护类型
操作	操作动作：编辑，删除

如图 1-2 示，在导航栏中选择“策略配置>安全设置>WEB 防护>防护策略”，进入防护策略的配置界面。点击“新建”弹框进入防护策略配置界面。

图1-2 防护策略配置界面

表1-2 防护策略配置界面详细描述表

标题项	说明
名称	策略名称
源地址	策略匹配的源地址
目的地址	策略匹配的目的地址
服务端口	HTTP服务的端口默认80
域名	服务的域名，可选项
描述	策略描述
启用	策略状态
防护配置	策略启用的防护类型

说明

Web 防护的优先级是精确访问控制、规则防护、防盗链、CSRF 攻击防护、CC 攻击防护、网页防篡改、应用隐藏，在未阻断情况下依次防护。

1.2.2 精确访问控制

精确访问控制是指用户可以根据自己的防护需求，自行定义一些防护规则，用于控制客户端的访问。这些规则不同于引擎规则，主要是基于 HTTP 协议头部的检测规则，可以实现黑白名单、封禁特定的 URL 等功能。

在导航栏中选择“策略配置>安全设置>WEB 防护>防护策略”，点击“新建”进入防护策略配置界面，在防护配置中选择“精确访问控制”标签页进入精确访问控制配置页面。如图 1-3 所示，界面显示信息的含义如表 1-3 所示。

图1-3 精确访问控制配置界面

表1-3 精确访问控制配置界面详细描述表

标题项	说明
启用	启用禁用精确访问控制
ID	规则ID
匹配条件	规则匹配条件
处理动作	精确访问规则处理动作：允许，拒绝
日志级别	日志级别
描述	精确访问规则描述
操作	操作动作：编辑，删除

如图 1-4 所示，在精确访问控制页面。点击“新建”弹框进入精确访问控制规则配置页面。各个配置项的含义如表 1-4 所示。

图1-4 精确访问控制规则配置界面

表1-4 精确访问控制规则配置界面详细描述表

标题项	说明
检测字段	匹配的检测字段
匹配方式	匹配的方式
匹配内容	匹配的内容
处理动作	动作：允许，拒绝
不再继续安全检查	其它WAF安全模块是否继续检查报文
日志级别	日志级别设置
描述	规则描述
启用	开启禁用规则

1.2.3 规则防护

支持多种类型攻击防护（规则分类）

- HTTP 协议检查。
- SQL 注入攻击防护。
- XSS 攻击防护。
- 目录遍历防护。
- 恶意扫描与爬虫防护。

- 木马防护。
- 敏感信息泄漏防护。
- 会话劫持防护。
- 文件上传防病毒扫描。
- 其它攻击防护（命令执行，代码执行，文件包含、会话固定、HTTP 响应拆分等相关规则）

在导航栏中选择“策略配置>安全设置>WEB 防护>防护策略”，点击“新建”进入防护策略配置界面，在防护配置中选择“规则防护”标签页进入规则防护配置页面。如图 1-5 所示，界面显示信息的含义如表 1-5 所示。

图1-5 规则防护配置界面

表1-5 规则防护配置界面详细描述表

标题项	说明
启用	开启关闭规则防护
日志	开启关闭日志
防护等级	默认规则库模板选择
防护类型	规则库自定义规则选择

如图 1-6 所示，在规则防护配置界面点击“防护类型”后面的蓝色超链接，弹框出现防护类型配置页面。

图1-6 防护类型配置界面

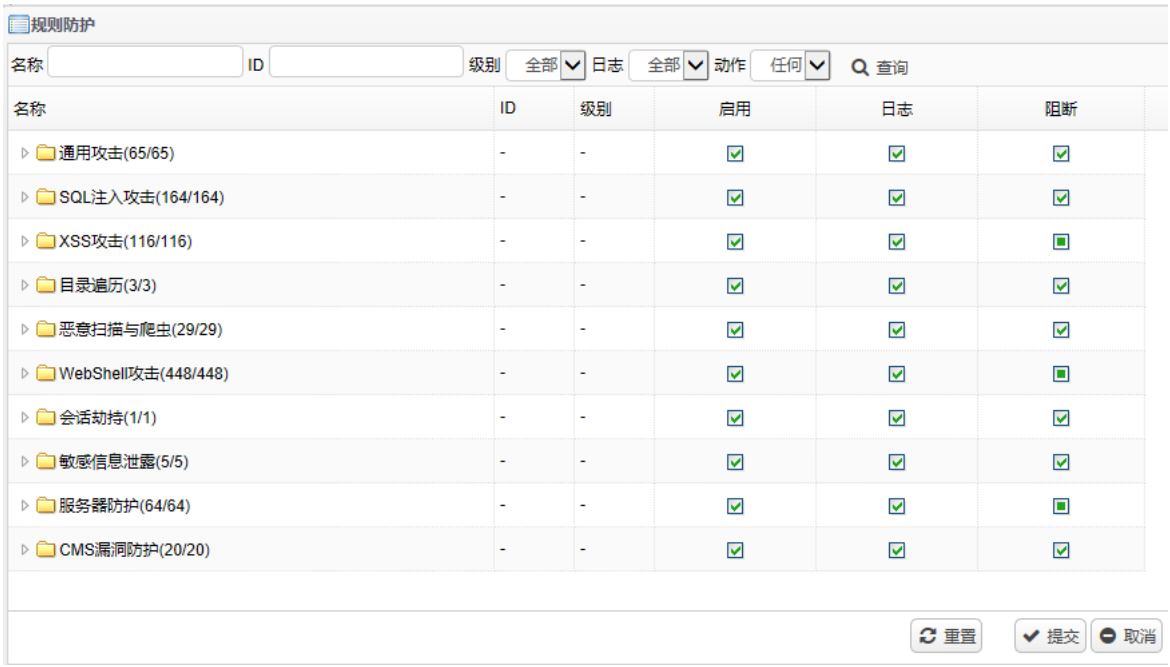


表1-6 防护类型配置界面详细描述表

标题项	说明
名称	勾选需要开启防暴力破解功能的服务
ID	防暴力破解的检测周期
级别	攻击次数，达到阈值触发防暴力破解记录攻击事件
启用	启用禁用规则
日志	启用禁用日志记录
阻断	阻断数据

1.2.4 防盗链

盗链是指某些网站自己并没有存储内容，其资源，比如图片和文件，都是通过技术手段从其它网站盗取的。防盗链也就是禁止其它网站盗用本网站的链接，这样不仅可以避免对本网站利益的损害，还可以减轻服务器的负担。

WEB 防护通过检查 HTTP 请求头部的 referer 字段来判断是否为盗链行为。该字段会存储访问目的网页的来源网页，如果该字段不为空，且其值不是允许的入口时，就认为是盗链。

防盗链支持全站防盗链、对指定的 URL 防盗链和对指定的文件类型防盗链。

如图 1-7 所示，在防护策略配置界面选择“防盗链”标签页，进入防盗链配置页面。

图1-7 防盗链配置界面

表1-7 防盗链配置界面详细描述表

标题项	说明
启用	启用禁用防盗链功能
防护范围	范围：全站，指定URL，指定文件类型
站点白名单	白名单站点
处理动作	动作：允许，拒绝
日志级别	日志级别设定

1.2.5 CSRF 攻击防护

CSRF 攻击可在受害者毫不知情的情况下以受害者名义伪造请求发送给受攻击站点，从而在并未授权的情况下执行在权限保护之下的操作。通过对 http 头中 referer 字段的检查，检测并防护此类攻击。通过部署 WEB 应用防火墙并对所保护的服务器配置 CSRF 防御功能，包括防护的 url 及允许访问的 referer，可以有效防止网站受到 CSRF 攻击。

如图 1-8 所示，在防护策略配置界面选择“CSRF 攻击防护”标签页，进入 CSRF 攻击防护配置页面。

图1-8 CSRF 攻击防护配置界面

如图 1-9 所示，在 CSRF 攻击防护页面。点击“新建”弹框出现 CSRF 攻击防护规则配置页面。

图1-9 CSRF 攻击防护配置界面

表1-8 CSRF 攻击防护配置界面详细描述表

标题项	说明
防护的URL	被保护的URL
允许的来源URL	允许的URL
处理动作	动作：允许，拒绝
日志级别	日志级别设定
启用	启用禁用规则

1.2.6 CC 攻击防护

CC 攻击是一种针对 HTTP 服务的 DDOS 攻击，攻击者通过代理服务器或者肉鸡向受害主机不停地发送大量请求包，消耗 HTTP 服务器资源，拖慢甚至瘫痪受害主机，从而影响正常的 HTTP 访问。CC 攻击防护支持全站防护和对指定的 URL 进行防护。

如图 1-10 所示，在防护策略配置界面选择“CC 攻击防护”标签页，进入 CC 攻击防护配置页面。

图1-10 CC 攻击防护配置界面

表1-9 CC 攻击防护配置界面详细描述表

标题项	说明
启用	启用禁用CC攻击防护
防护范围	范围：全站，指定URL
检测时长	CC防护检测周期
访问次数	访问指定url的次数
处理动作	动作：允许，拒绝
日志级别	日志的级别设定

1.2.7 网页防篡改

如图 1-11 所示，在防护策略配置界面选择“网页防篡改”标签页，进入网页防篡改配置页面。

图1-11 网页防篡改配置界面

表1-10 网页防篡改配置界面详细描述表

标题项	说明
启用	启用禁用网页防篡改功能
起始URL	被保护的URL
例外URL	不检测的URL
处理动作	动作：允许，拒绝
日志级别	日志的级别设定

1.2.8 应用隐藏

应用隐藏是指隐藏 HTTP 服务端返回的某些信息，比如服务器版本，服务器端编码方式以及某些特定的错误码等，这些信息很可能被攻击者利用从而进行有针对的攻击，比如服务器版本为 Apache/2.4.23，那么如果攻击者知道这个版本的漏洞，就能轻易的进行攻击。

应用隐藏支持屏蔽 HTTP 头部的 Server 字段和 X-Powered-By 字段，Server 字段是服务器版本信息，比如 Apache/2.4.23，X-Powered-By 字段是服务器端编码方式，比如 PHP/5.5.38。

此外，还支持 4xx（客户端错误码）和 5xx（服务端错误码）错误码的检查和返回内容的替换。服务器返回的错误信息往往包含服务器的重要信息，这些信息也很可能被攻击者利用。当返回码是 4xx 或 5xx 时，设备会将返回页面替换为一个不包含任何关键信息的预设页面，避免服务器信息的泄漏。

对于某个被防护的站点，Server 字段的屏蔽、X-Powered-By 字段的屏蔽、4xx 错误码的替换以及 5xx 错误码的替换，都支持单独开启关闭。

如图 1-12 所示，在防护策略配置界面选择“应用隐藏”标签页，进入应用隐藏配置页面。

图1-12 应用隐藏配置界面

表1-11 应用隐藏配置界面详细描述表

标题项	说明
启用	启用禁用应用隐藏功能
隐藏Server信息	隐藏服务器信息
隐藏X-powered-By	隐藏服务器信息
替换客户端出错页面（4xx）	替换（4xx）指定默认页面
替换服务器端出错页面（5xx）	替换（5xx）指定默认页面
日志级别	日志解绑设定

1.3 规则库

如图 1-13 所示，在导航栏中选择“策略配置>安全设置>WEB 防护>规则库”，进入规则库查询界面。

图1-13 规则库查询界面

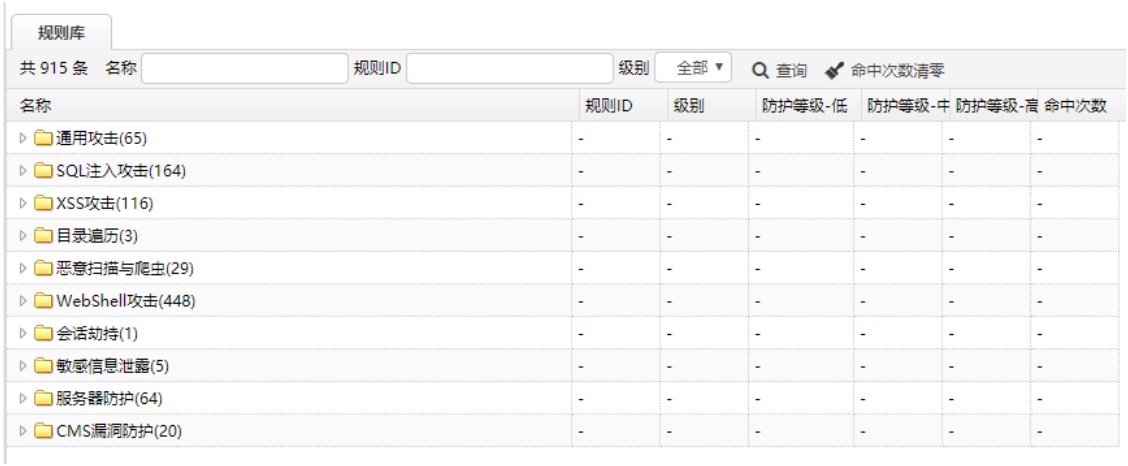


表1-12 服务配置界面详细描述表

标题项	说明
命中次数清零	点击清空规则命中次数
名称	规则名称
规则ID	规则的ID
级别	规则的级别
防护等级	规则的防护等级
命中次数	规则的命中次数

1.4 防篡改网页缓存

如图 1-14 所示，在导航栏中选择“策略配置>安全设置>WEB 防护>防篡改网页缓存”，进入防篡改网页缓存配置界面。

图1-14 防篡改网页缓存配置界面

表1-13 防篡改网页缓存配置界面详细描述表

标题项	说明
缓存清理	清理勾选的缓存URL

目 录

1 风险扫描 1
1.1 端口扫描 1
1.1.1 端口扫描简介 1
1.1.2 端口扫描任务 1
1.1.3 端口扫描结果 2
1.2 弱密码扫描 3
1.2.1 弱密码扫描简介 3
1.2.2 弱密码扫描任务 3
1.2.3 字典管理 4

1 风险扫描

1.1 端口扫描

1.1.1 端口扫描简介

端口扫描采用多线程方式对指定 IP 地址段(或单机)进行开发端口检测，支持自定义端口和模糊端口功能，提供单次端口扫描和周期性端口扫描方式，扫描结果支持同步资产信息中。

1.1.2 端口扫描任务

如图 1-1 所示，在导航栏中选择“策略配置>安全设置>风险扫描>端口扫描>端口扫描任务”，进入端口扫描任务的配置界面。点击“新建”创建扫描任务。

图1-1 端口扫描任务配置界面

表1-1 端口扫描任务界面详细描述表

标题项	说明
任务名称	自定义任务名称
地址项目	被扫描的网络地址，支持主机，网段，范围设置
资产发现同步	勾选后扫描结果可同步更新资产信息
端口	支持自定义端口和模糊端口方式，模糊端口只支持TCP端口
扫描类型	单次扫描或定期扫描时间配置
任务描述	自定义任务描述

1.1.3 端口扫描结果

如图 1-2 所示，在导航栏中选择“策略配置>安全设置>风险扫描>端口扫描>端口扫描结果”，进入端口扫描结果的配置界面。

图1-2 端口扫描结果界面

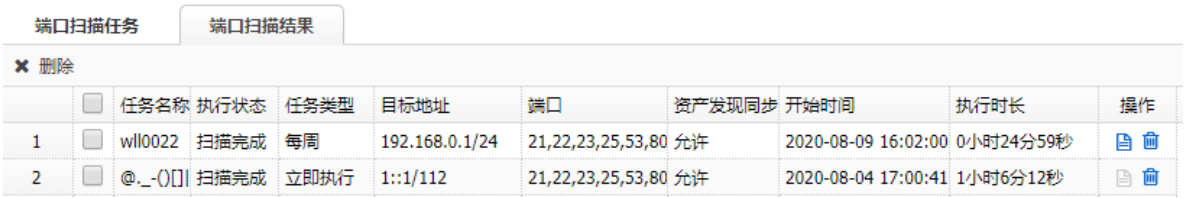


表1-2 端口扫描结果详细描述表

标题项	说明
删除	删除端口扫描历史结果
任务名称	端口扫描任务名称
执行状态	端口扫描任务执行状态
任务类型	端口扫描任务周期，比如：单次、每周等
目的地址	端口扫描IP范围
端口	端口扫描端口范围
资产发现同步	展示资产发现同步勾选状态
开始时间	端口扫描开始时间
执行时长	端口扫描执行时长
操作	可删除端口扫描历史记录 可点击详细查看详细端口扫描历史记录

1.2 弱密码扫描

1.2.1 弱密码扫描简介

弱密码扫描采用多线程方式对指定 IP 地址段(或单机)进行弱密码检测，支持自定义字典功能，提供单次弱密码扫描和周期性弱密码扫描方式，扫描服务包括: ftp、ssh、telnet、imap、smtp、pop3、mssql、mysql、postgres、rlogin、vnc。

1.2.2 弱密码扫描任务

如图 1-3 所示，在导航栏中选择“策略配置>安全设置>风险扫描>弱密码扫描>扫描任务”，进入弱密码扫描任务的配置界面。点击“新建”创建扫描任务。

图1-3 弱密码扫描任务配置界面

表1-3 弱密码扫描任务界面详细描述表

标题项	说明
任务名称	自定义任务名称
项目地址	被扫描的网络地址。支持主机、网段、范围设置，支持IPv6地址。
服务	扫描的服务项

扫描方式	根据字典库内容选择不同扫描方式
空密码检测	开启关闭空密码检测功能
用户名和密码相同检测	开启关闭用户名和密码相同检测功能
扫描类型	单次扫描或定期扫描时间配置
任务描述	自定义任务描述

1.2.3 字典管理

如图 1-4 所示，在导航栏中选择“策略配置>安全设置>风险扫描>弱密码扫描>字典管理”，进入自定义字典的配置界面。点击“新建”创建字典。

图1-4 字典配置界面

表1-4 字典配置界面详细描述表

标题项	说明
名称	字典的名称
描述	字典的描述
自定义字典	字典内容

目 录

1 系统管理 ····· 1-1
1.1 授权管理 ····· 1-1
1.1.1 授权管理概述 ····· 1-1
1.1.2 手动导入许可证 ····· 1-1
1.1.3 非经 SDK 配置方法 ····· 1-2
1.2 升级管理 ····· 1-2
1.2.1 升级管理概述 ····· 1-2
1.2.2 手动升级 ····· 1-3
1.2.3 自动升级 ····· 1-5
1.2.4 补丁升级 ····· 1-6
1.2.5 升级记录查看 ····· 1-7
1.3 系统重启 ····· 1-8
1.3.1 系统重启 ····· 1-8
1.3.2 恢复出厂设置 ····· 1-8
1.4 配置文件 ····· 1-9
1.5 配置管理员 ····· 1-10
1.5.1 管理员概述 ····· 1-10
1.5.2 配置管理员 ····· 1-10
1.5.3 查看在线管理员 ····· 1-11
1.5.4 查看被阻断用户 ····· 1-12
1.6 管理设定 ····· 1-13
1.6.1 管理设定配置 ····· 1-13
1.6.2 管理员外部认证 ····· 1-14
1.6.3 三权分立 ····· 1-15
1.7 时间设定 ····· 1-19
1.8 快速配置 ····· 1-21
1.8.1 快速配置概述 ····· 1-21
1.8.2 快速配置向导 ····· 1-21
1.9 系统诊断工具 ····· 1-25
1.9.1 Ping ····· 1-25
1.9.2 Traceroute ····· 1-26
1.9.3 TCP Syn ····· 1-26
1.10 抓包工具 ····· 1-27

1.11 服务器管理 ····· 1-29
1.11.1 服务器管理概述 ····· 1-29
1.11.2 FTP 服务器的配置 ····· 1-29
1.11.3 邮件服务器的配置 ····· 1-31
1.12 典型配置举例 ····· 1-32
1.12.1 三权分立的配置举例 ····· 1-32
1.12.2 管理员认证典型配置举例 ····· 1-36
1.12.3 Ping 配置举例 ····· 1-38
1.12.4 Traceroute 配置举例 ····· 1-40
1.12.5 TCP Syn 配置举例 ····· 1-42

1 系统管理

1.1 授权管理

1.1.1 授权管理概述

可以通过手动点击导入许可证来对应用监控升级服务/URL 分类库升级服务/恶意 URL 分类库升级服务、入侵防御/病毒防护升级服务以及非经 SDK 功能进行授权。如图 1-1 所示。

图1-1 导入许可证图

1.1.2 手动导入许可证

通过菜单“系统管理 > 系统维护 > 授权管理”，进入如图 1-2 所示页面。配置项含义如表 1-1 所示。

图1-2 手动导入许可证页面

表1-1 手动导入许可证配置项含义描述表

标题项	说明
导入许可证	对系统软件进行授权。
非经SDK功能授权	对非经SDK功能进行授权后，需要在命令行config视图下配置rzx gam-audit | (enable/disable)选择开启或关闭

1.1.3 非经 SDK 配置方法

由于老版本非经配置过于繁琐，为满足市场需求，增加非经 SDK 功能使用授权特性。对非经 SDK 功能进行授权后，需要在命令行 config 视图下配置如下命令选择开启或关闭：

rzx gam-audit | (enable/disable)

图1-3 非经 SDK 配置命令

```
AK220-主主2(config)# rzx gam-audit
  disable  Switch disable
  enable   Switch enable
AK220-主主2(config)# rzx gam-audit
```

说明

R6611P02 及之后版本新增非经 SDK 功能，为了兼容 R6611P02 之前版本非经功能，web 页面老的无线非经功能保留，已经使用老的无线非经功能的用户可以升级新版本继续兼容使用，也可以修改到新的 SDK 功能使用（需要进行授权才能使用），新用户建议使用新的 SDK 功能，操作比较简单，只需授权激活，命令行 config 视图下配置开启命令（rzx gam-audit enable）

未导入非经 SDK 功能使用授权的 license 时无法启用非经 SDK 功能，授权过期后会自动关闭非经 SDK 功能，再次重新授权后不会自动开启非经 SDK 功能，需要手工开启。

使用 SDK 功能需要设备可以和外网互通，设备可以通过 ping 百度测试；设备 mac 地址在设备铭牌上有体现，同时对应设备的第一个接口 mac 地址

1.2 升级管理

1.2.1 升级管理概述

可以通过手动本地升级系统软件版本和特征库，也可自动升级 URL 分类特征库和应用控制特征库。

对于已发布的版本，通过上传升级热补丁，可以在不影响系统运行的情况下，完成对设备版本的缺陷进行修复，热补丁正确加载后补丁文件立即生效。如图 1-4 所示。

图1-4 升级页面总图

1.2.2 手动升级

通过菜单“系统管理 > 系统维护 > 系统升级”，进入如图 1-5 所示页面。各个配置项含义如表 1-2 所示。

图1-5 手动升级页面

表1-2 手动升级各个配置项含义描述表

标题项	说明
系统软件	升级系统软件版本或热补丁。 升级系统软件版本，升级后需要重启设备方可生效； 升级热补丁，不需重启设备即可生效。
应用控制特征库	升级应用控制特征库。
入侵防御特征库	升级入侵防御特征库
病毒防护特征库	升级病毒防护特征库

1.2.3 自动升级

通过菜单“系统管理 > 系统维护 > 系统升级”，进入如图 1-6 所示页面，页面中的红色圈选部分为配置项。各个配置项含义如表 1-3 所示。

图1-6 自动升级页面

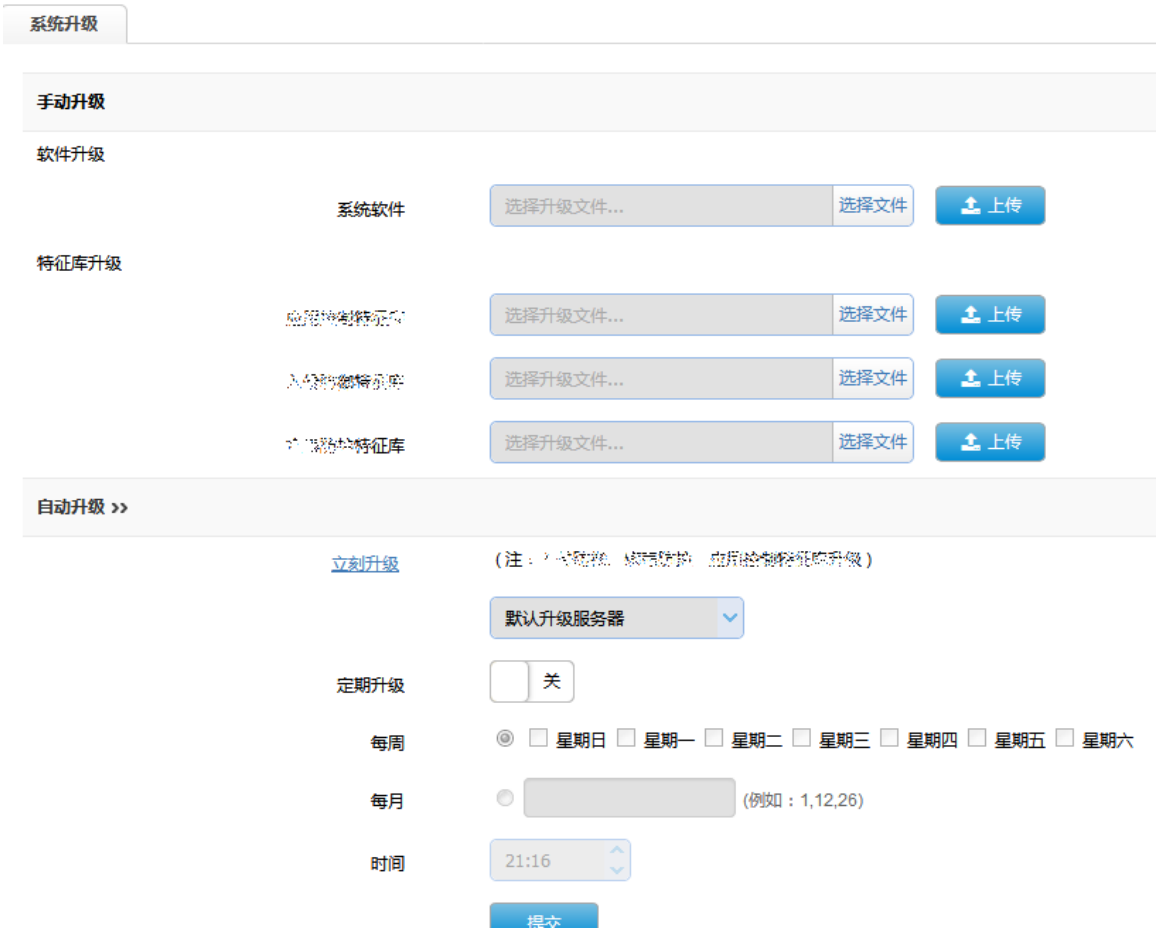


表1-3 自动升级各个配置项含义描述表

标题项	说明
默认升级服务器	升级服务器设为默认升级服务器。
指定升级服务器	设置升级服务器地址。
定期升级	启用定期自动升级。
每周	按星期定期自动升级。
每月	按每月日期自动升级，日期间以“,”分隔。
时间	每次自动升级的当天时间。

点击<提交>按钮，提交自动升级配置。

点击<立即升级>按钮，可立即更新特征库，无需等到自动升级指定时间点，首次配置设备时建议进行一次立即升级。

说明

采用自动升级功能时，需要在设备上设定有效的 DNS。

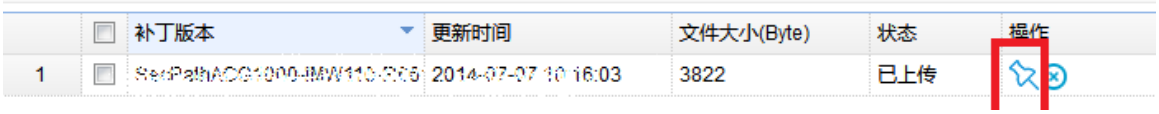
1.2.4 补丁升级

通过菜单“系统管理>系统维护>系统升级”，进入如图 1-7 所示界面；单击“系统软件”中的“浏览”按钮，选择待上传的补丁文件，单击“上传”按钮上传补丁文件。

图1-7 补丁升级上传界面

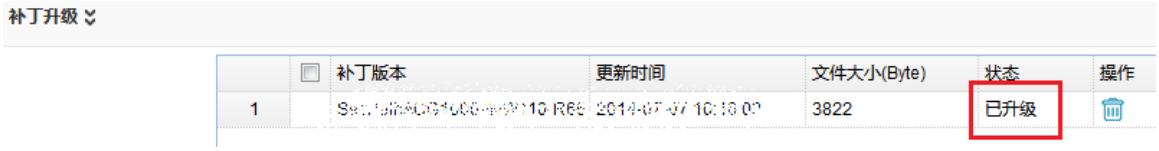
单击“补丁升级”进入如图 1-8 所示界面；选中要升级的补丁版本，单击“”按钮进行补丁升级。

图1-8 补丁升级界面



升级成功后，版本状态显示为“已升级”，如图 1-9 所示界面。

图1-9 升级成功界面



单击“”按钮可对已升级的补丁进行卸载，热补丁卸载成功后，在补丁升级框中该补丁显示已上传。

图1-10 卸载成功界面

单击“”按钮可对已上传或已卸载的补丁进行删除，热补丁删除成功后，在补丁升级框中该补丁被删除；正在加载的补丁不允许删除。

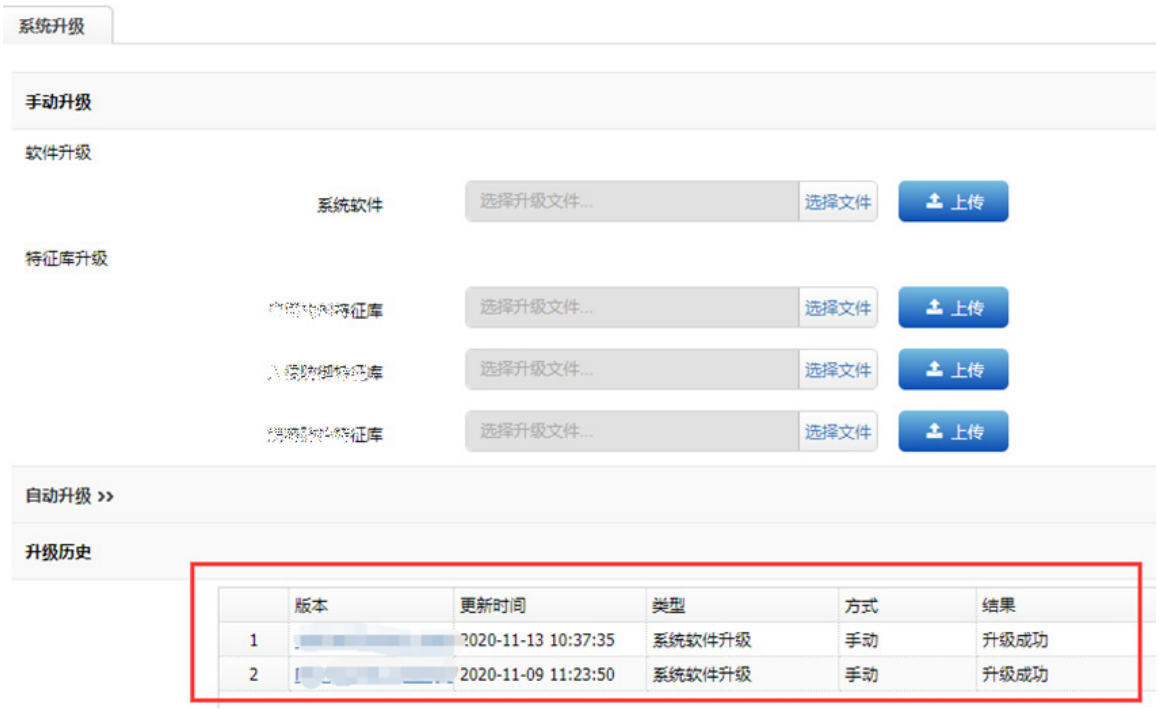
说明

- 上传热补丁数量限制为 5 个。
- 为了保证补丁操作进程堆栈安全，补丁的操作时间间隔为 30S。
- 补丁文件必须以“.pat”作为扩展名，不支持中文。

1.2.5 升级记录查看

通过菜单“系统管理 > 系统维护 > 系统升级”，进入如图 1-11 所示页面，通过页面中的红色圈选部分，查看升级记录。

图1-11 查看升级记录



1.3 系统重启

1.3.1 系统重启

通过菜单“系统管理 > 系统维护 > 系统重启”，进入如图 1-12 所示页面，选择“系统重启”。

图1-12 系统重启页面

点击<提交>按钮，重启系统。

1.3.2 恢复出厂设置

通过菜单“系统管理 > 系统维护 > 系统重启”，进入如图 1-13 所示页面，选择“恢复出厂设置”。

图1-13 恢复出厂设置

点击<提交>按钮，恢复出厂设置。

1.4 配置文件

通过菜单“系统管理 > 系统维护 > 配置维护”，进入如图 1-14 所示页面，管理配置文件。各个配置项的含义如表 1-4 所示。

图1-14 配置文件管理页面

表1-4 配置文件管理各个配置项含义描述表

标题项	说明
系统配置导入	从本地主机中选择要导入的配置文件上传至设备。
系统配置导出	将保存的配置导出至本地主机。 注：导出的文件是UTF-8编码模式。
双备份配置	可以选择拷贝主配置文件到备份配置文件，或恢复备份配置文件到主配置文件。恢复备份配置后，需重启系统配置才可生效，重启前请勿保存配置。

1.5 配置管理员

1.5.1 管理员概述

设备出厂的默认配置自动创建了一个超级管理员用户 admin，使用这个账号，可以登录设备对设备进行配置，包括配置其它的管理员，每个管理员都有它的管理地址。

1.5.2 配置管理员

管理员是登录设备对设备进行配置管理的用户。通过菜单“系统管理 > 系统设定 > 管理员”，进入管理员界面，如图 1-15 所示。各个显示项含义如表 1-5 所示。

图1-15 本地管理员显示界面

表1-5 管理员界面显示信息描述表

标题项	说明
用户名	管理员的名称。
角色	有两种管理员角色： • 管理员角色； • 审计员角色。
认证类型	有三种认证类型： • 本地认证； • RADIUS 认证； • LDAP 认证。
描述	管理员的描述信息。
管理地址	管理员的管理地址，只有在这个范围内的地址才能通过此管理员来管理设备。

点击图 1-15 的<新建>按钮，可以进入如图 1-16 所示的新建管理员界面。各个配置项的含义如表 1-6 所示。

图1-16 新建管理员界面

表1-6 管理员的详细配置描述表

配置项	说明
用户名	管理员的名称。
描述	针对管理员的说明。
认证类型	选择创建的账号的认证类型，选择第三方RADIUS和LDAP服务器认证时需提前配置服务器。
密码	用户对应的密码，最少6个字符。
确认密码	对输入的密码进行确认输入。
本地	在本地进行管理员认证。
RADIUS	如果在用户组中包含了用户名、RADIUS服务器，如果用户本地存在则在本地进行认证，若不存在则发往RADIUS服务器进行认证。
LDAP	如果在用户组中包含了用户名、LDAP服务器，如果用户本地存在则在本地进行认证，若不存在则发往LDAP服务器进行认证。
管理IP	管理IP栏可以配置授权地址，最多可配置3个。缺省情况下，从任何地址都可以登录设备进行配置管理。
角色	管理员的角色，可选取管理员或审计员。

1.5.3 查看在线管理员

通过菜单“系统管理 > 系统设定 > 管理员”，然后再点击“在线信息”标签页，可以查看正在管理设备的管理员，如图 1-17 所示。各个显示项的含义如表 1-7 所示。

图1-17 显示在线管理员

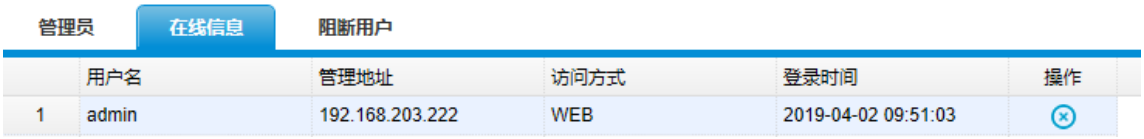


表1-7 在线管理员界面显示信息描述表

标题项	说明
用户名	管理员的名称。
管理地址	管理员登录的IP地址。
访问方式	管理员可以通过以下几种方式来管理设备： • WEB • CONSOLE • SSH • TELNET • DataCenter
登录时间	管理员登录的时间。
操作	点击删除图标可以根据需要强制管理员下线 。

说明

通过直接连接设备串口登录的管理员无法强制管理员下线。

1.5.4 查看被阻断用户

通过菜单“系统管理 > 系统设定 > 管理员 > 阻断用户”，然后再点击“阻断用户”标签页，可以查看当前被阻断登录的用户信息，如图 1-18 所示。缺省情况下，阻断时间为一分钟，点击操作下面的删除图标可立即解除阻断。

图1-18 查看阻断用户页面

1.6 管理设定

1.6.1 管理设定配置

通过菜单“系统管理 > 系统设定 > 管理设定”，进入管理设定配置页面，如图 1-19 所示。各个配置项的含义如表 1-8 所示。

图1-19 管理设定配置页面

表1-8 管理设定配置项含义描述表

标题项	说明
实时保存配置	是否实时的保存配置，通过web管理方式管理时，配置修改后将自动保存。
管理员唯一性检查	是否检查管理员的唯一性，即是否只允许一个管理员登录。
管理员双因子认证	管理员双因子认证，开启后当使用https方式登录设备时需要有经过授权的Ukey+合法账号才能登录设备。 Ukey管理软件：对Ukey进行初始化激活 Ukey客户端软件：通过客户端软件将设备端生成的用户证书导入Ukey

标题项	说明
最大登录尝试次数	允许管理员登录失败后重新登录的次数。
登录失败阻断间隔	管理员登录失败允许再次登录的间隔时间。
页面超时时间	页面超时时间，如操作时间超过该值页面将自动退出。
web在线管理员	同时web在线的管理员的最大个数。
管理员认证方式	选择管理员认证方式（本地认证或外部认证）。 • 本地认证：使用设备本地管理员账号密码登录设备； • 外部认证：选择外部服务器进行外部认证。
HTTPS端口	设备HTTPS管理端口，默认为443，可修改为1024-65534之间未被系统使用的端口
HTTP端口	设备HTTP管理端口，默认为80，可修改为1024-65534之间未被系统使用的端口
TELNET端口	设备TELNET管理端口，默认为23，可修改为1024-65534之间未被系统使用的端口
SSH端口	设备SSH管理端口，默认为22，可修改为1024-65534之间未被系统使用的端口

1.6.2 管理员外部认证

1. 管理员外部认证概述

目前系统管理员支持认证方式：radius 服务器认证方式、LDAP 服务器认证方式，这两种认证方式都需要在设备上建立管理员账户，对于本地用户名密码校验是合理的，但是对于其它两种外部认证方式，本地保存用户名对于认证过程没有作用，不仅会增加维护复杂性，还会导致账户外泄，增加安全隐患。

为了更好的提高设备可维护性，在 RADIUS 服务器校验方式、LDAP 服务器校验方式中，不再需要配置用户名。

本功能具有如下功能点：

- 全局设定支持管理员认证方式切换：本地认证、外部服务器认证；
- 在保留现有本地认证方式的基础上增加支持外部服务器认证。

2. 配置管理员外部认证

通过菜单“系统管理 > 系统设定 > 管理设定”，进入如图 1-20 所示页面。在该页面上可以配置管理员外部认证的相关功能。各个配置项含义如表 1-9 所示。

图1-20 管理员外部认证配置页面

表1-9 管理员认证方式配置项含义表

标题项	说明
管理员认证方式	选择管理员认证方式（本地认证或外部认证）。 • 本地认证：使用设备本地管理员账号密码登录设备； • 外部认证：选择外部服务器进行外部认证。
认证服务器	选择管理员外部登录时使用哪种认证服务器（Radius或Ldap）。
radius/ldap	选择认证服务器对象。
服务器异常开启本地认证	选择外部认证时可以选择服务器异常是否开启本地认证，默认为开启状态。

1.6.3 三权分立

1. 三权分立概述

设备的三权分立主要为一些资质审核公司要求管理员互相制约互相监控的功能。

三权分立共有四种管理员，分别为原内嵌管理员 admin，三权分立后 account 用户、authority 用户、audit 用户，可以分别有以下权限：

- admin 账户：内嵌管理员用户，三权模式下由 authority 用户对其进行功能授权，以实现对功能点权限为只读或可读写，进而对功能进行操作控制。
- account 用户：account 负责账号创建，可新建自定义系统管理员；可进行操作日志查看。
- authority 用户：可以系统管理员功能模块授权，模块细分读写或只读模式。
- audit 用户：审核管理员可对用户权限监控及操作日志查看。

2. 模式切换

通过菜单“系统管理>系统设定>管理设定>模式切换”，进入模式切换页面，进行普通模式到三权模式的切换，如图 1-21 所示。该动作不可逆，提交后，当前配置页面将退出登录状态。

图1-21 模式切换配置页面

说明

- 账户新建只能由 accout 用户新建。
- 切换三权模式需慎重，配置界面不可回切。
- 所有用户初始密码均为 admin。
- 三权模式下系统管理员 admin 的缺省密码在切换为三权模式前已经更改，请使用修改后的密码进行登录，此次登录不会强制要求修改密码。
- 账号管理员、权限管理员以及审计员在首次登录设备时，系统要求强制修改默认密码，且不能与默认密码相同。

进入三权模式后，将自动生成三个管理员账号：account，authority，audit。

Account（账号管理员）登录后，可以进行管理员账号的新建、删除，以及对账号管理员操作日志的查看，如图 1-22 所示。同时，该账号可编辑自身账号的管理员名称及密码。

图1-22 账号管理员配置页面

authority（权限管理员）登录后，可以进行管理员账号的权限进行新建、删除、编辑，以及对权限管理员操作日志的查看。同时，该账号可编辑自身账号的管理员名称及密码，如图 1-23、图 1-24所示。

权限状态为“待分配”表示当前该管理员账号未授予权限，权限管理员分配权限后，状态将变为“已分配”。

图1-23 权限管理员配置页面

图1-24 权限管理员权限编辑页面

Audit（审核员）登录后，可以进行对当前管理员账号权限状态的审计，以及对所有账号操作日志的审计查看，如图 1-25、图 1-26 所示。同时，该账号可编辑自身账号的管理员名称及密码。

图1-25 审核员审核页面

		用户名	角色	认证类型	描述	管理地址	权限状态	操作
1		anonym	系统管理员	本地		0.0.0.0/0	待分配	
2		admin	系统管理员	本地	admin	0.0.0.0/0	已分配	
3		test	系统管理员	本地	test		已分配	
4		account	账号管理员	本地		0.0.0.0/0	内置	
5		authority	权限管理员	本地		0.0.0.0/0	内置	
6		audit	审核员	本地		0.0.0.0/0	内置	

图1-26 审核员操作日志查看页面

	时间	日志级别	操作管理员	操作员IP	详细信息	日志内容
1	2019-03-26 19:23:07	通知	admin	192.168.7.140	用户 192.168.7.140 使用 telnet operate 结果 success	con terminal
2	2019-03-26 19:23:05	通知	admin	192.168.7.140	用户 192.168.7.140 使用 telnet operate 结果 success	en
3	2019-03-19 13:49:26	通知	admin	192.168.200.36	用户 192.168.200.36 使用 telnet operate 结果 success	ena
4	2019-03-19 13:47:00	通知	admin	192.168.200.36	用户 192.168.200.36 使用 telnet operate 结果 success	ena
5	2019-03-19 12:55:13	通知	admin	192.168.203.222	用户 192.168.203.222 使用 web operate 结果 success	reboot
6	2019-03-19 12:55:07	通知	admin	192.168.203.222	用户 192.168.203.222 使用 WEB 修改 结果 成功	修改 重启 配置

1.7 时间设定

配置系统时间有两种方式，手动配置和通过配置 NTP 同步获得系统时间。通过菜单“系统管理 > 系统设定 > 时间设定”进入时间设定页面，如图 1-27 所示。各个配置项的含义如表 1-10 所示。

图1-27 设置系统时间页面

表1-10 时间设定配置项描述表

标题项	子标题项	说明
系统当前时间	系统时间	显示当前系统时间。
	时区	选择系统当前时区。
手动设定系统时间	系统时间	手动设置的系统时间。
	时区	手动设置的时区。
NTP时间设定	主服务器	NTP主服务器。
	备服务器	NTP备服务器。
	同步间隔	NTP每次同步间隔，单位：分钟。

1.8 快速配置

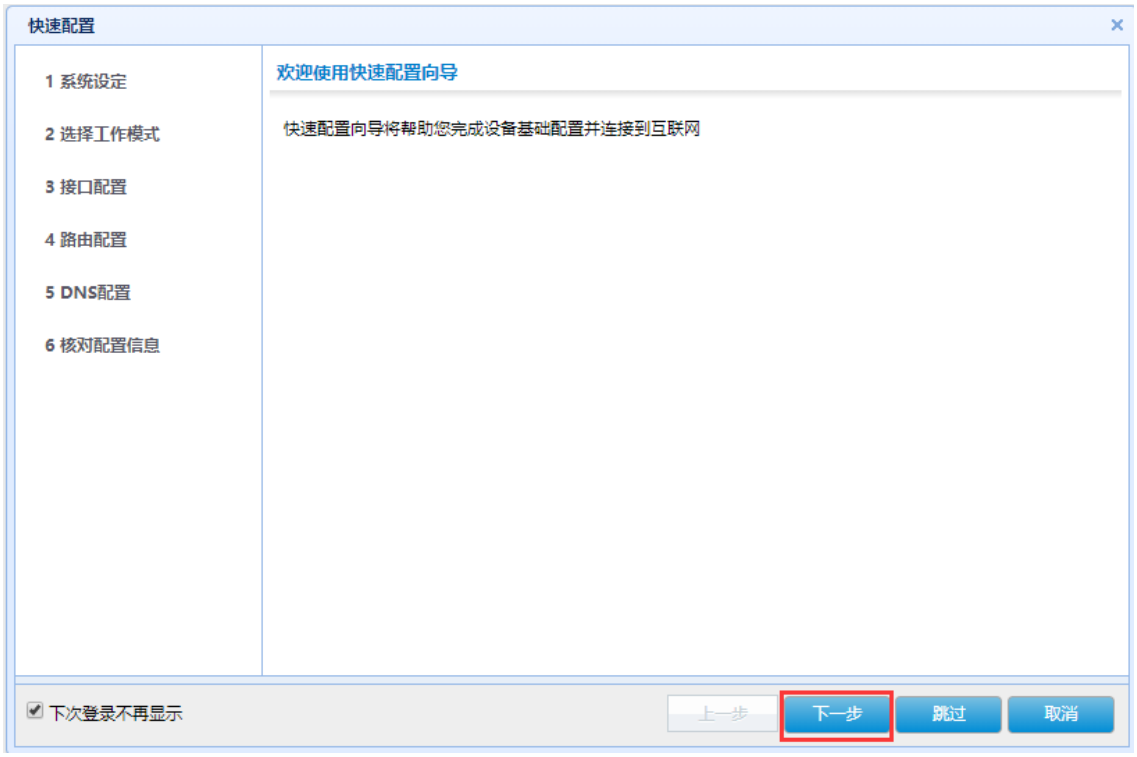
1.8.1 快速配置概述

首次登录设备时会自动弹出快速配置框，也可以通过“系统管理 > 系统设定 > 快速配置”手动打开。通过快速配置向导的提示可以设置主机名称、系统时间等，根据网络拓扑以及应用场景选择工作模式，并完成接口、路由、DNS 等功能的快速配置，可以在快速配置的引导下实现网关模式、网桥模式、旁路模式的快速配置。

1.8.2 快速配置向导

首次登录设备后，系统自动弹出“快速配置”页面，在欢迎界面单击“下一步”。如图 1-28 所示。

图1-28 快速配置向导欢迎界面

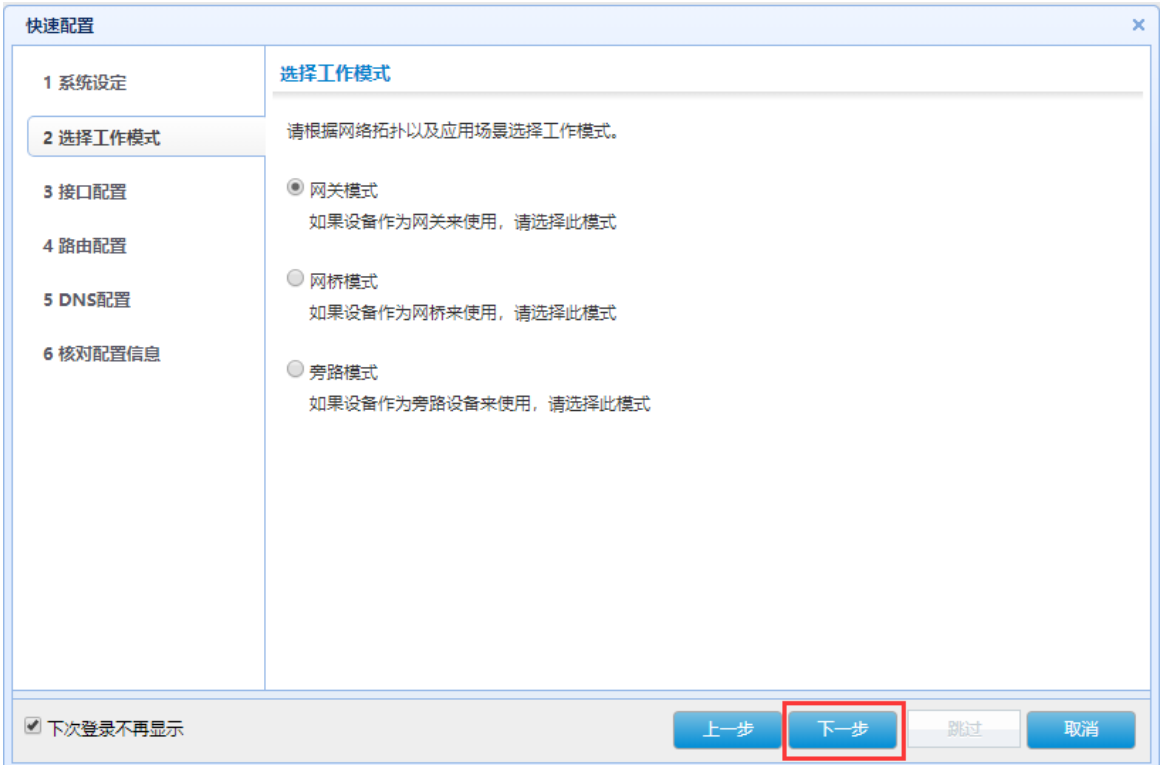


在系统设定中完成主机名称、时间以及默认策略的配置，并单击“下一步”。如图 1-29 所示。

图1-29 快速配置 1-系统设定

根据组网需求选择工作模式，并单击“下一步”。如图 1-30 所示。

图1-30 快速配置 2-选择工作模式

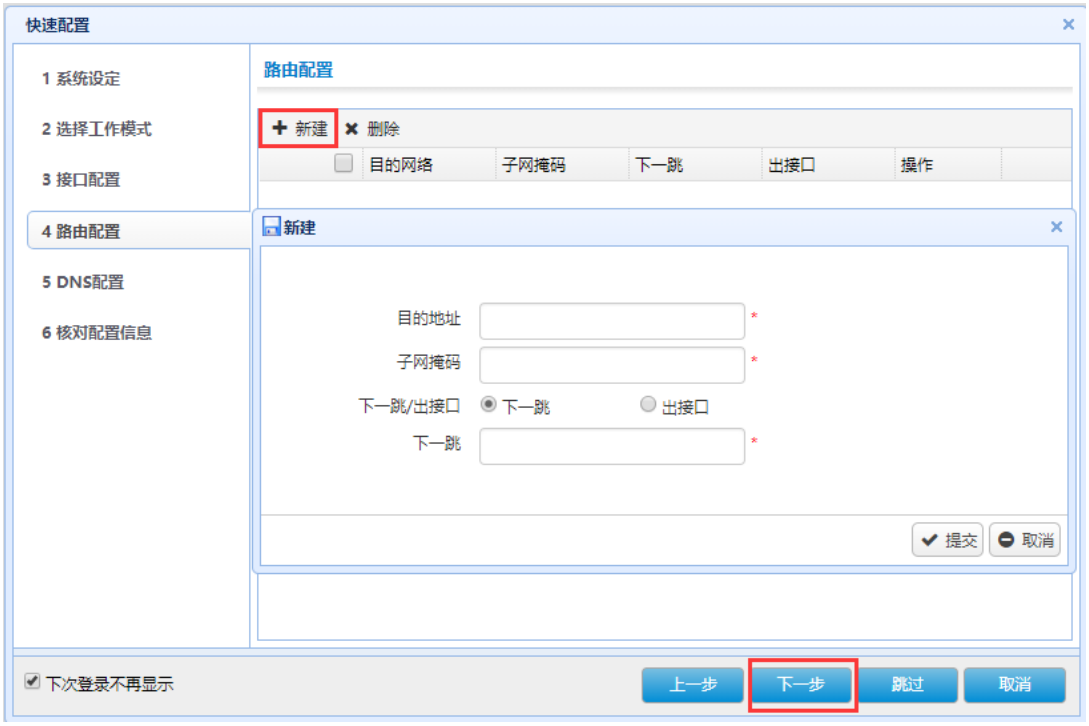


根据组网需求配置接口相关内容，比如接口 IP，管理方式等，然后单击“下一步”。如图 1-31 所示。

图1-31 快速配置 3-接口配置

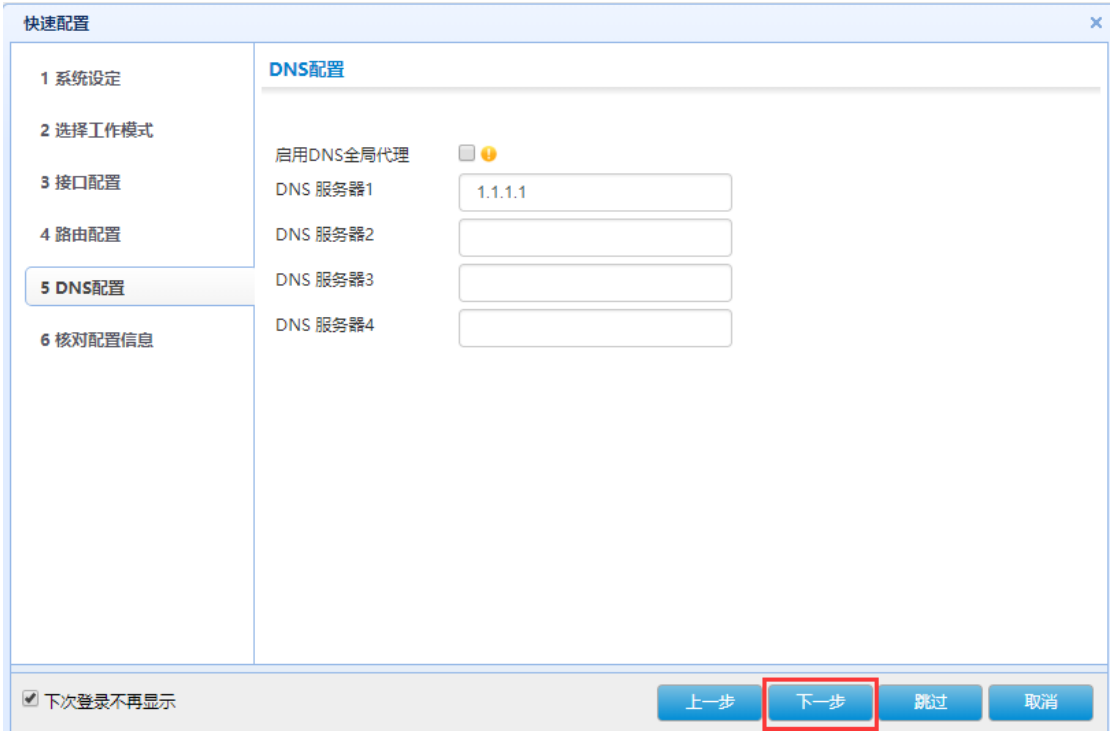
在路由配置界面单击“添加”，在新建框中填写路由相关配置，单击“提交”，然后单击“下一步”。如图 1-32 所示。

图1-32 快速配置 4-路由配置



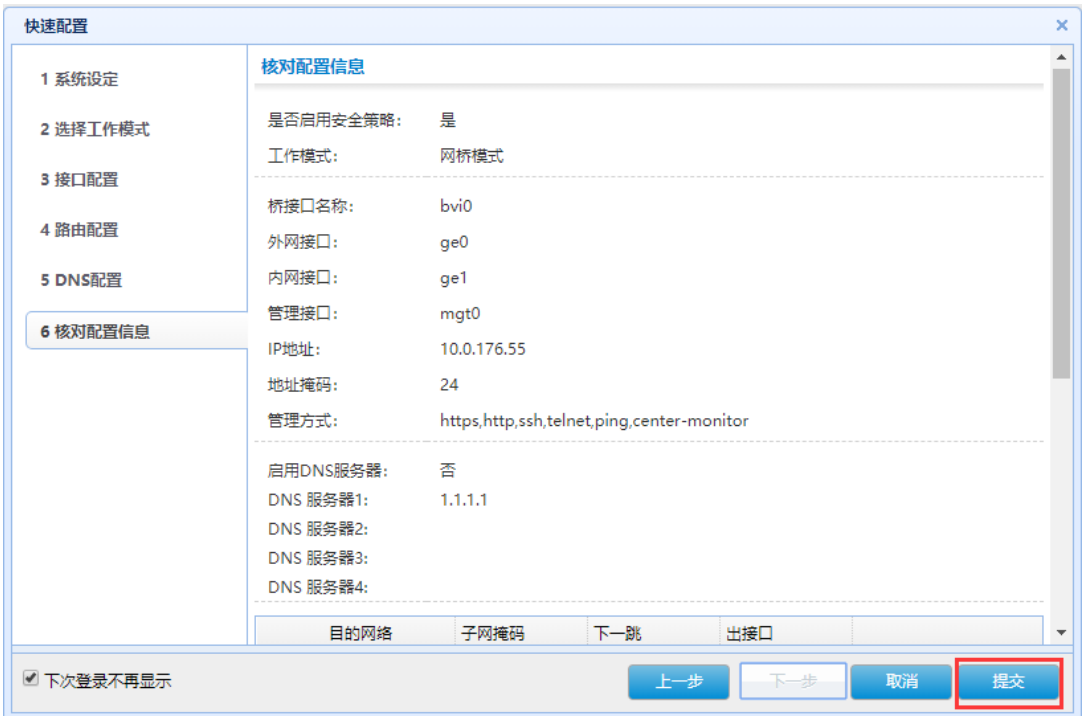
在 DNS 配置页面配置 DNS 服务器地址，并根据需求选择启用 DNS 全局代理。如图 1-33 所示。

图1-33 快速配置 5-DNS 配置



核对配置信息，确认配置无误后，单击“提交”，即可完成快速配置。如图 1-34 所示。

图1-34 快速配置 6-核对配置信息



说明

- 首次登录设备时会自动弹出快速配置页面，忽略或者完成后，下次不再弹出。
- 如果已经在快速配置的页面选择了“下一次登录不再提示”，则后续登录不会弹出快速配置页面。
- 可以通过“系统管理 > 系统设定 > 快速配置”手动开启快速配置向导。

1.9 系统诊断工具

1.9.1 Ping

通过菜单“系统管理 > 系统维护 > 系统诊断工具 > Ping”，进入如图 1-35 所示页面。各个配置项的含义如表 1-11 所示。

图1-35 Ping 页面

表1-11 Ping 各个配置项含义描述表

标题项	说明
目的地址	需要ping的IP地址，或域名。
探测包数目	发送探测包的数量。

标题项	说明
探测包大小	每个探测包的大小。
Ping结果	显示ping包返回的结果。

1.9.2 Traceroute

通过菜单“系统管理 > 系统维护 > 系统诊断工具 > Traceroute”，进入如图 1-36 所示页面。各个配置项的含义如表 1-12 所示。

图1-36 Traceroute 页面

表1-12 Traceroute 各个配置项含义描述表

标题项	说明
目的地址	需要探测的地址。
探测方式	可以选择UDP/ICMP两种探测方式。
Traceroute探测结果	显示探测结果。

1.9.3 TCP Syn

通过菜单“系统管理 > 系统维护 > 系统诊断工具 > TCP Syn”，进入如图 1-37 所示页面。各个配置项的含义如表 1-13 所示。

图1-37 TCP Syn 页面

表1-13 TCP Syn 各个配置项含义描述表

标题项	说明
目的地址	需要探测的地址。
端口	TCP端口号。
探测包数目	探测包的发送数量。
TCP Syn包探测结果	显示探测结果。

1.10 抓包工具

通过菜单“系统管理 > 系统维护 > 抓包工具”，进入如图 1-38 所示页面。各个配置项的含义如表 1-14 所示。

图1-38 抓包工具页面

表1-14 抓包工具各个配置项含义描述表

标题项	说明
接口	要抓取报文的接口。
协议	抓取报文的协议类型。
源IP	抓取报文的源IP地址，全零或空表示任意地址。
源端口	抓取报文的源端口号，零或空表示任意端口号。
目的IP	抓取报文的目的IP地址，全零或空表示任意地址。
目的端口	抓取报文的目的端口号，零或空表示任意端口号。
抓取新建会话	抓取新建连接的前N个报文，取值为0~1024。
应用	根据应用协议抓取报文。

抓取结束后，抓取的报文文件将以.pcap 格式保存，在如图 1-39 所示的页面中显示，并提供导出。各个配置项的含义如表 1-15 所示。

图1-39 文件列表页面

表1-15 文件列表各个配置项含义描述表

标题项	说明
文件名称	抓取报文的文件名称。
文件大小	抓取报文的文件大小。
结束时间	抓取报文的结束时间。
操作	可删除或导出对应文件。

1.11 服务器管理

1.11.1 服务器管理概述

系统告警支持邮件外发功能，报表管理支持邮件外发和 FTP 外发，可通过服务器管理页面配置邮件服务器和 FTP 服务器来实现邮件外发及 FTP 外发。

1.11.2 FTP 服务器的配置

通过菜单“系统管理>服务器管理>FTP 服务器”，进入 FTP 服务器配置页面，如图 1-40 所示。

图1-40 FTP 服务器配置页面

页面的详细说明如表 1-16 所示。

表1-16 FTP 服务器配置详细说明

项目	说明
服务器地址/域名	发送的FTP服务器的IP地址或域名
FTP服务器端口	FTP服务器的端口
用户名	登录FTP服务器的用户名
密码	登录FTP服务器的密码

单击<验证用户和密码>验证 FTP 服务器的用户名和密码访问是否成功，并显示验证结果，如图 1-41 所示。

图1-41 FTP 用户名和密码验证成功

1.11.3 邮件服务器的配置

通过菜单“系统管理>服务器管理>邮件服务器”，进入邮件服务器配置页面，如图 1-42 所示。

图1-42 邮件服务器配置页面

页面的详细说明如表 1-17 所示。

表1-17 邮箱服务器配置详细说明

项目	说明

项目	说明
发件人地址	发件人邮箱地址
邮箱服务器	发送地址的邮箱服务器
服务器端口	服务器端口
SSL	选中后可设置SSL协议端口号
smtp 服务器身份验证	配置smtp 服务器身份验证的用户名、密码，如果不需要验证可不选。
测试邮箱有效性	检查配置是否正确，正确则会收到测试邮件

1.12 典型配置举例

1.12.1 三权分立的配置举例

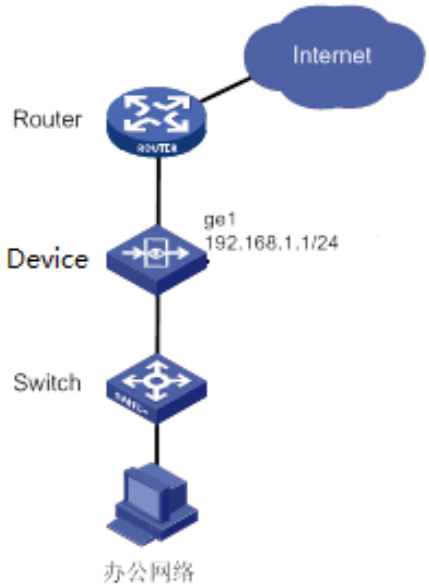
1. 组网需求

如图 1-43 所示，设备以透明模式串接在某公司网络的核心交换机和出口路由器之间，具体应用需求如下：

- 设备开启三权模式，设备使用的 IP 地址为 192.168.1.1/24。
- 需要 authority 用户给 admin 用户分配权限，分别为分配：网络配置、网络优化、对象管理、上网行为管理的执行权限。

设备 account 用户新建自定义用户为 test，只分配监控统计、日志查询、上网行为管理的只读权限。

图1-43 三权分立配置案例组网图



2. 配置步骤

如图 1-44 所示，设备管理模式为“三权模式”，并点击<提交>。

图1-44 更改为三权分立模式

如图 1-45 所示，使用 account 用户新建管理员 test。

图1-45 使用 account 用户新建管理员 test

如图 1-46 所示，使用 authority 用户对 admin 用户进行读写授权。

图1-46 使用 authority 用户对 admin 用户进行读写授权

如图 1-47 所示，使用 authority 用户登录，点击 admin 账号后 图标，分配：网络管理、策略配置的执行权限，将全选只读勾掉，在此页面上点击<提交>。

图1-47 分配执行权限

如图 1-48 所示，使用 authority 用户登录，点击 test 账号后 图标，分配数据中心的只读权限，在此页面上点击<提交>。

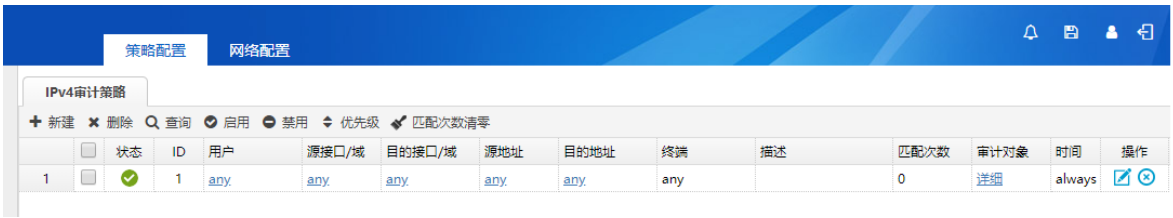
图1-48 分配：监控统计、数据中心权限

3. 验证配置

验证 admin 用户权限

如图 1-49 所示，使用 admin 用户对策略配置、网络配置等授权功能模块可读可写可执行。

图1-49 admin 用户权限验证



如图 1-50 所示，使用自定义 test 用户对数据中心的授权只读模块只有只读权限。

图1-50 自定义 test 用户权限验证

如图 1-51 所示，audit 用户登录只有审核员权限。

图1-51 audit 审核员登录

1.12.2 管理员认证典型配置举例

1. 组网需求

管理员可以访问设备登录页面，如果配置外部认证方式，使用外部服务器内的账号可以登录设备。

- 设备到外部服务器可达。
- 如果设备到外部服务器不可达，开启服务器异常进行本地认证，使用本地账号可以登录。

2. 配置步骤

(1) 配置 RADIUS 服务器。如图 1-52 所示。

图1-52 RADIUS 服务器配置页面

(2) 配置管理员外部 radius 认证。如图 1-53 所示。

图1-53 管理员 radius 认证配置

3. 验证配置

(1) 配置完成后，用户访问设备登录页面，使用 radius 服务器内的账号密码登录设备，登录成功，使用本地账号密码登录，提示账号密码错误。

(2) “服务器异常开启本地认证”开关选择“开启”时，如果设备与服务器无法通讯，使用本地账号密码可以登录成功。

(3) “服务器异常开启本地认证”开关选择“关闭”时，如果设备与服务器无法通讯，使用本地账号无法登录设备。

说明

- 管理员外部认证功能只针对管理员模式生效，三权模式不支持。
- 外部认证时，只支持选择服务器对象且只能选择一个，不支持同时选择多个，不支持服务器对象组。

1.12.3 Ping 配置举例

1. 组网需求

检测设备网络是否畅通。

2. 配置步骤

按照图 1-54 所示配置。

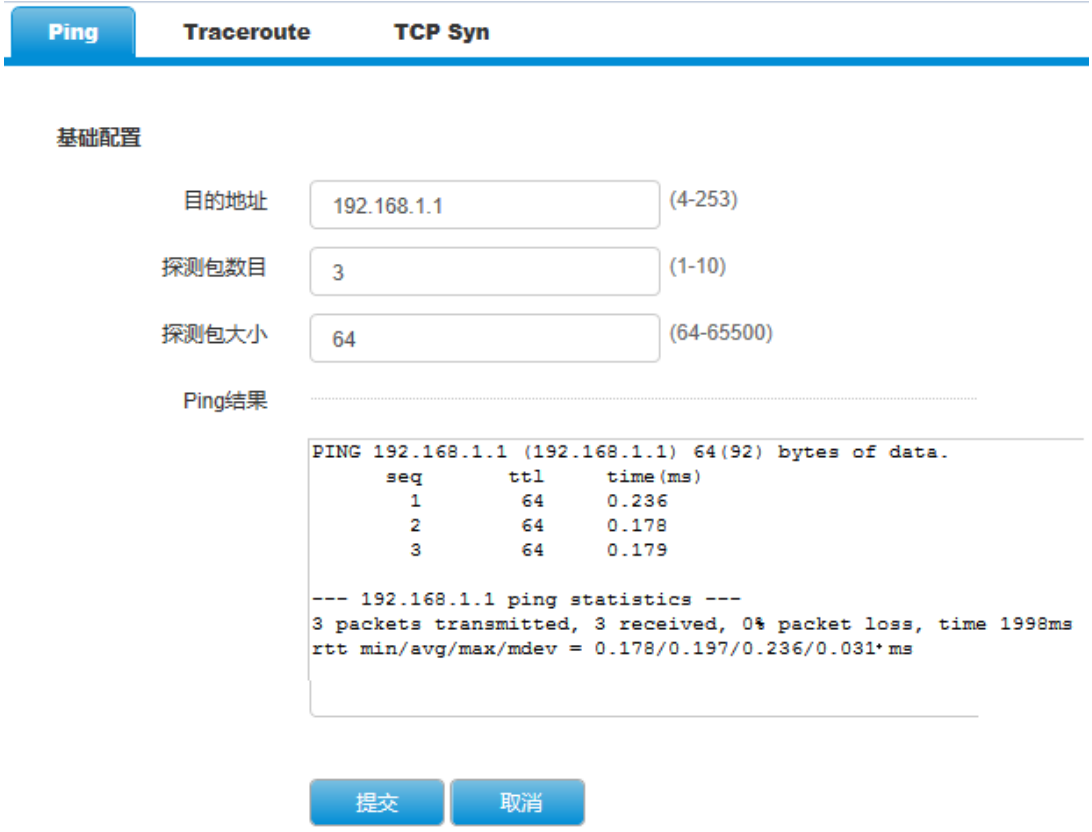
图1-54 配置 Ping

点击<提交>按钮，提交配置。

3. 验证配置

查看诊断结果。如图 1-55 所示。

图1-55 Ping 结果



1.12.4 Traceroute 配置举例

1. 组网需求

检测设备网络是否畅通。

2. 配置步骤

按照图 1-56 所示配置。

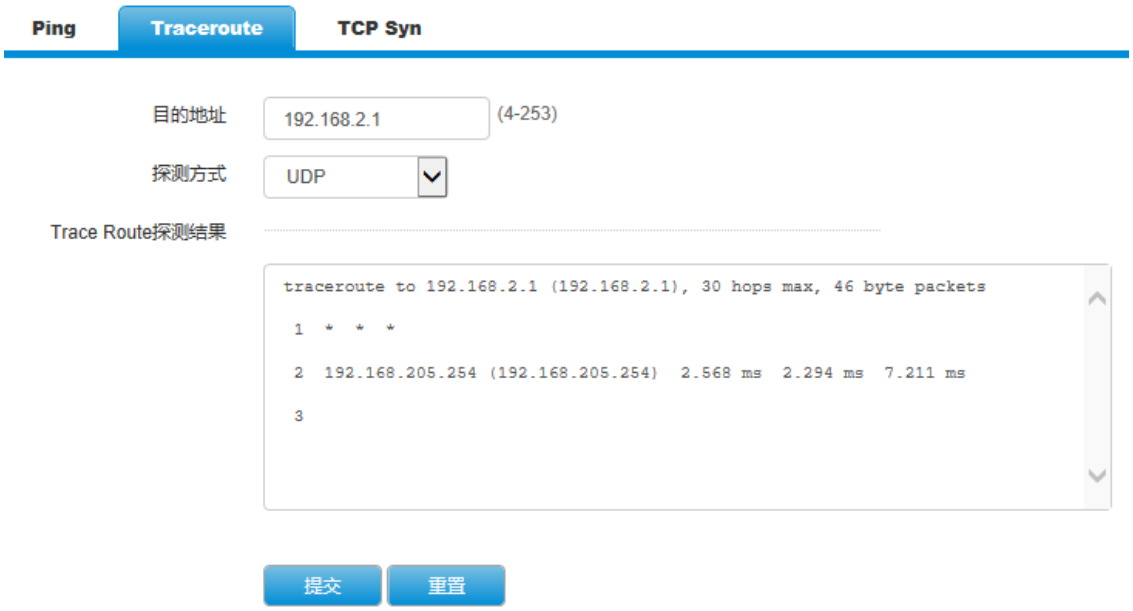
图1-56 配置 Traceroute

点击<提交>按钮，提交配置。

3. 验证配置

查看诊断结果。如图 1-57 所示。

图1-57 Traceroute 结果



1.12.5 TCP Syn 配置举例

1. 组网需求

检测设备网络是否畅通。

2. 配置步骤

按照图 1-58 所示配置。

图1-58 配置 TCP Syn

点击<提交>按钮，提交配置。

3. 验证配置

查看诊断结果。如图 1-59 所示。

图1-59 TCP Syn 结果

目 录

1 管理端口漂移 ····· 1-1
1.1 管理端口漂移介绍 ····· 1-1
1.2 管理端口漂移的配置 ····· 1-1
1.3 配置举例 ····· 1-2
1.3.1 管理端口漂移的配置举例 ····· 1-2

1 管理端口漂移

1.1 管理端口漂移介绍

管理端口漂移的作用在于能够即时方便的修改 http，https，ssh，telnet 四种协议的通讯端口。更换相应的协议端口号后，原有的链接将会断开。

1.2 管理端口漂移的配置

通过菜单“系统管理 > 系统设定 > 管理设定”，进入如图 1-1 所示的页面。在该页面上，可以修改 http、https、ssh、telnet 四种协议的通讯端口，各个配置项的含义如表 1-1 所示，管理设定的其它配置项含义详见“系统管理”章节中管理设定模块。

图1-1 修改 http，https，ssh，telnet 四种协议的通讯端口

表1-1 http，https，ssh，telnet 四种协议的通讯端口配置项含义

标题项	说明
HTTPS端口	HTTPS管理端口，默认443端口
HTTP端口	HTTP管理端口，默认80端口
TELNET端口	TELNET管理端口，默认23端口
SSH端口	SSH管理端口，默认22端口

说明

http 默认端口号是 80，https 默认端口号是 443，ssh 默认端口号是 22，telnet 默认端口号是 23。它们可以配置的端口号是 1024-65535 之间未被系统其它进程使用的端口号。

1.3 配置举例

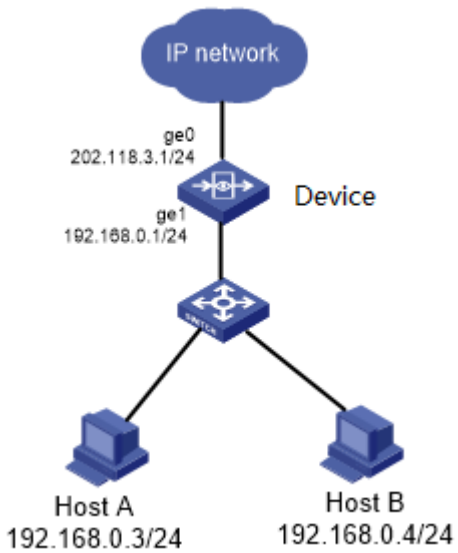
1.3.1 管理端口漂移的配置举例

1. 组网需求

各设备接口及主机的 IP 地址和掩码如图 1-2 所示。测试用户 HostA，HostB 通过设备正常上网。

2. 组网图

图1-2 管理端口漂移的配置案例组网图



3. 配置步骤

(1) 按照组网图组网。

(2) 通过菜单“系统管理 > 系统设定 > 管理设定”，按照如图 1-3 所示修改 http，https，ssh，telnet 四种协议的通讯端口。

图1-3 修改 http，https，ssh，telnet 四种协议的通讯端口

点击<提交>按钮，提交配置。

4. 验证配置

在浏览器中输入 http://192.168.2.176:8080，使用修改后的 http：8080 管理端口登录设备验证是否生效，如图 1-4。

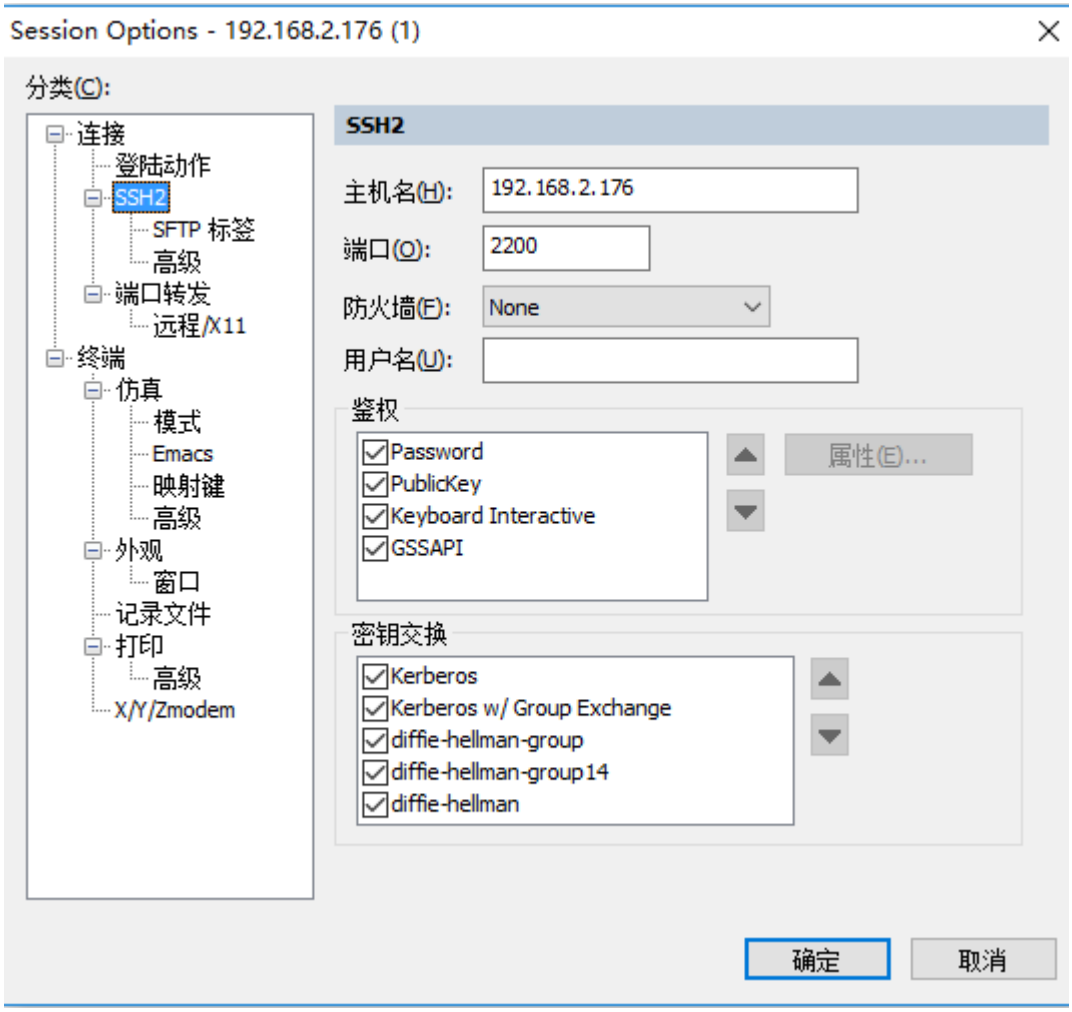
图1-4 验证使用 http：8080 登录设备

在浏览器中输入 https://192.168.2.176:4430，使用修改后的 https：4430 管理端口登录设备验证是否生效，如图 1-5。

图1-5 验证使用 https：4430 登录设备

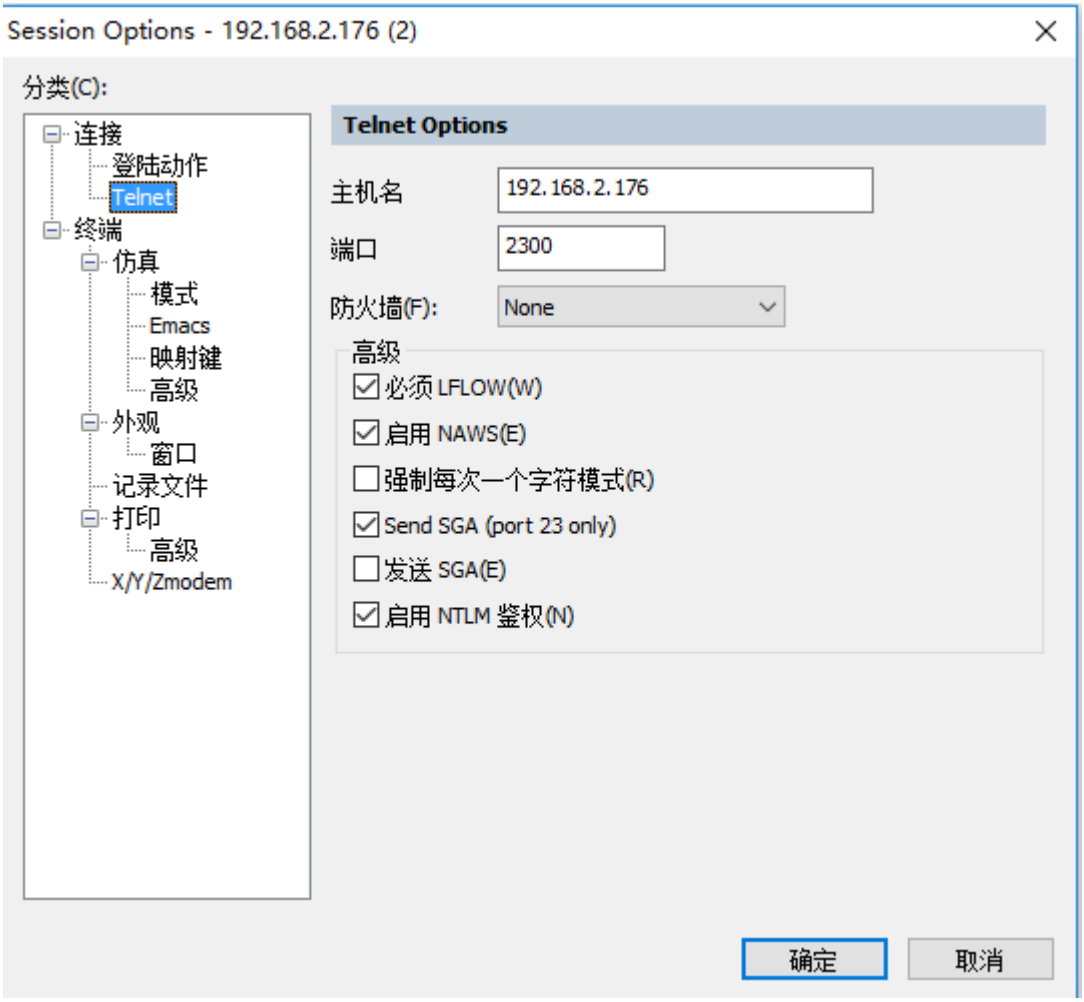
使用修改后的 ssh：2200 管理端口登录设备验证是否生效，如图 1-6。

图1-6 验证使用 ssh：2200 登录设备



使用修改后的 telnet：2300 管理端口登录设备验证是否生效，如图 1-7。

图1-7 验证使用 telnet：2300 登录设备



目 录

1 SNMP ····· 1-1
1.1 SNMP 简介 ····· 1-1
1.2 配置 SNMP ····· 1-1
1.3 配置 SNMP USM 用户 ····· 1-2
1.4 SNMP 典型配置举例 ····· 1-4
1.4.1 SNMP 典型配置举例 ····· 1-4

1 SNMP

1.1 SNMP简介

SNMP（Simple Network Management Protocol，简单网络管理协议），它是一个标准的用于管理IP 网络上节点的协议。由一组网络管理的标准组成，包含一个应用层协议（application layer protocol）、数据库模型（database schema）和一组资源对象。该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。现已从 V1 版本，更新至 V3 版本。SNMPv3 版本是基于用户的安全模型（USM）。较 V1、V2 版本认证更为安全。

本功能支持 V1 至 V3 版本。

本功能具有如下功能点：

- 能够对设备上支持的公有 MIB 节点进行查询和设置。
- 能够设置 TRAP 信息上报。
- 能够对设备上的私有 MIB 节点进行查询和设置。
- 支持 SNMP v1、v2c、v3 版本。
- 支持 Trap V1、v2c Notification、v2c Inform 版本。

1.2 配置SNMP

通过菜单“系统管理 > 系统设定 > SNMP 配置 > SNMP 配置”，进入如图 1-1 所示页面。在该页面上可以配置 SNMP 的相关功能。各个配置项含义如表 1-1 所示。

说明

- 使用 SNMP v3 版本管理设备比使用 SNMP v1、v2c 版本更安全，建议使用 SNMP v3 版本管理设备。
- v2c Notification 与 v2c Inform 发送 TRAP 信息是一样的，v2c Inform 是可靠传输，需要 SNMP 管理服务器进行响应。

图1-1 SNMP 配置页面

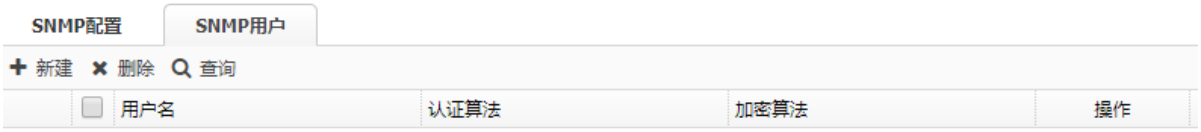
表1-1 SNMP 配置项含义表

标题项	说明
SNMP代理	开启或关闭SNMP功能，勾选为开启，不勾选为关闭。
版本	SNMP需要启用的版本选项，支持v1、v2c、v3版本。
TRAP版本	SNMP TRAP信息的版本选项，支持v1、v2c_notification、v2c_inform版本。
TRAP地址	SNMP TRAP报文的上报地址，TRAP地址可以设置为IPv4和IPv6地址。
位置	设备的位置信息，可输入0到255个字符。
读团体名	SNMP的读团体字，可输入6到256个字符，默认值为“default-public”（R6611P03之前版本，默认值改为“public”）。
写团体名	SNMP的写团体字，可输入6到256个字符，默认值为“default-private”（R6611P03之前版本，默认值改为“private”）。

1.3 配置SNMP USM用户

通过菜单“系统管理 > 系统设定 > SNMP 配置 > SNMP 用户”，进入如图 1-2 所示页面。在该页面上可以新建、编辑、删除、浏览 SNMP USM 用户。

图1-2 SNMP USM 用户概览页面



点击页面上的<新建>按钮，可以新建 USM 用户。新建页面如图 1-3 所示。各个配置项的含义如表 1-2 所示。

图1-3 USM 用户新建页面

表1-2 USM 用户配置项含义表

标题项	说明
用户名	USM用户的用户名称，可输入1到31个字符
认证	USM用户的认证方式，支持MD5、SHA和SHA256三种方式
认证密码	USM用户的认证密码，可输入8到31个字符，认证密码必须包括数字、字母以及字符(!@#$%',-.)
加密	USM用户的加密方式，支持DES和AES两种方式
加密密码	USM用户的加密密码，可输入8到31个字符，加密密码必须包括数字、字母以及字符(!@#$%',-.)

点击<提交>按钮，提交配置。提交配置后可在如图 1-4 所示的页面上查看配置的 USM 用户信息。

图1-4 USM 用户信息概览页面

点击<编辑>按钮，可对选中条目进行编辑。

点击<删除>按钮，可对选中条目进行删除。

1.4 SNMP典型配置举例

1.4.1 SNMP 典型配置举例

1. 组网需求

远端主机通过网络使用 MIB Browser 软件访问、监控、配置设备。

- 远端主机和设备网络可达。
- 主机端装有 MIB Browser 软件。

2. 组网图

图1-5 SNMP 组网图

3. 配置步骤

(1) 配置 SNMP。如图 1-6 所示。

图1-6 配置 SNMP

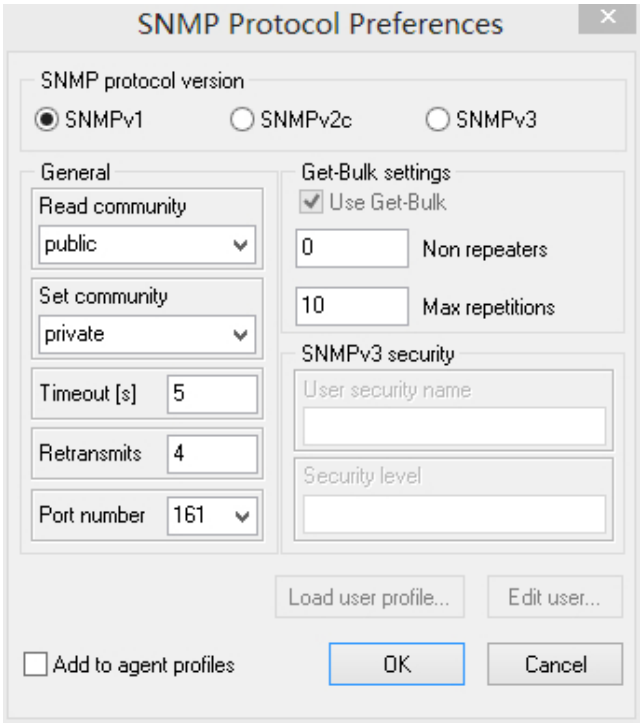
(2) 配置 USM 用户。如图 1-7 所示。

图1-7 USM 用户配置页面

(3) 主机配置 MIB Browser。

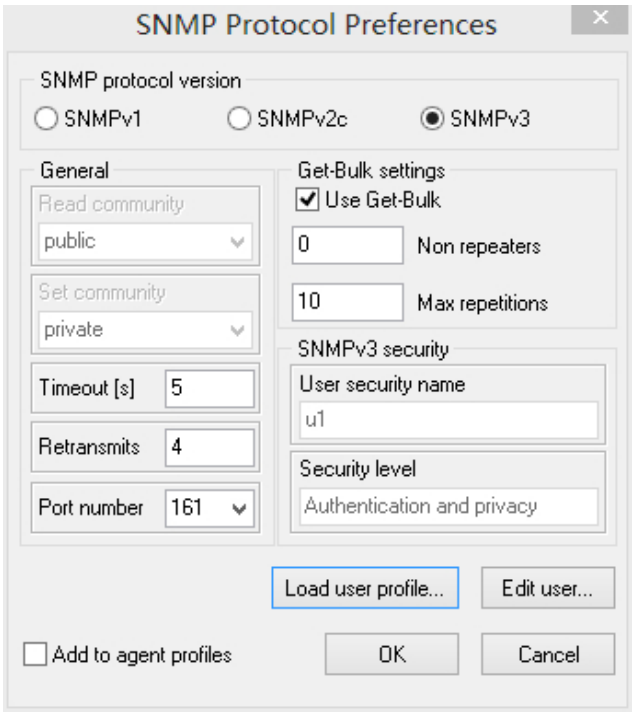
v1 或 v2 版本的 Mib Browser 的配置，如图 1-8 所示。

图1-8 MIB Browser 的 V1、V2 版本配置



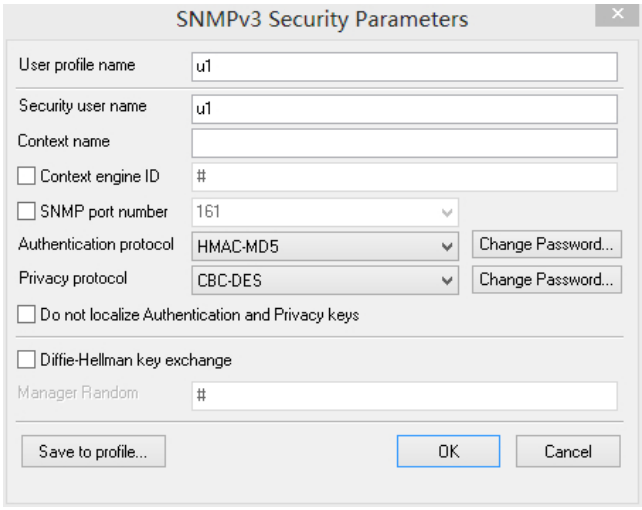
v3 版本的 Mib Browser 的配置，如图 1-9 所示。

图1-9 MIB Browser 的 V3 版本配置



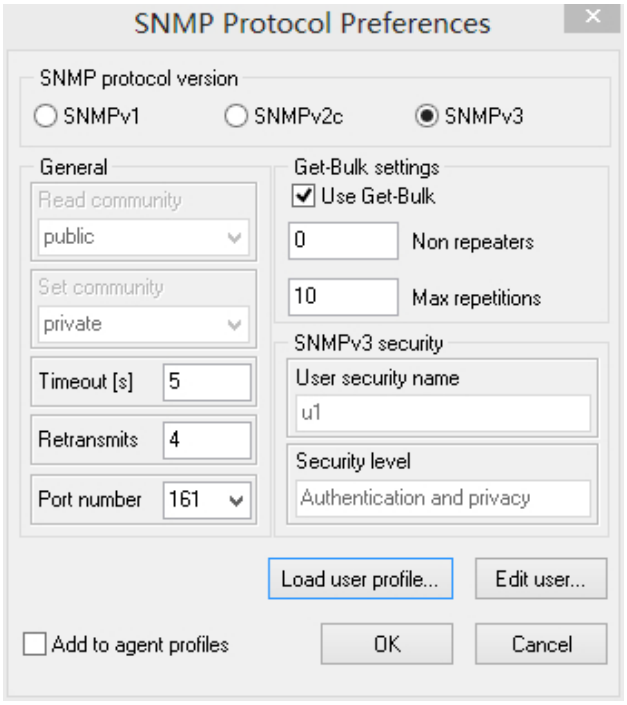
选择 load user profile，创建 USM 用户，如图 1-10 所示。

图1-10 创建 USM 用户



选择用户，主机端配置完成，如图 1-11 所示。

图1-11 选择 USM 用户



4. 验证配置

配置完成后，在主机端使用 MIB Browser 工具，对节点执行 get 或 set 操作，即可获取到对应的设备信息。

说明

- 在主机端的 MIB Browser 上只需要选择一种 SNMP 版本。
- 对于 SNMP 的 V1、V2 版本，在主机端的 MIB Browser 上配置的读命令字和写命令字，需要与设备上配置的相同，才能建立连接。
- 如果需要给主机主动发送 TRAP 报文，则需要在设备上配置 TRAP 地址。

目 录

1 日志……1-1
1.1 日志概述……1-1
1.1.1 日志的类型……1-1
1.1.2 日志的等级……1-2
1.1.3 日志信息输出……1-2
1.2 配置日志服务器……1-2
1.3 配置日志过滤……1-4
1.4 系统日志查询……1-5
1.4.1 系统日志查询……1-5
1.4.2 操作日志查询……1-7
1.5 控制日志查询……1-9
1.5.1 应用控制日志查询……1-9
1.5.2 恶意 URL 日志……1-13
1.6 审计日志查询……1-14
1.6.1 访问网站日志……1-14
1.6.2 IM 聊天软件日志……1-18
1.6.3 社区日志……1-21
1.6.4 搜索引擎日志……1-24
1.6.5 邮件日志……1-27
1.6.6 文件传输日志……1-29
1.6.7 娱乐/股票日志……1-32
1.6.8 协议审计日志……1-34
1.6.9 其它应用日志……1-36
1.7 安全日志查询……1-39
1.7.1 入侵日志……1-39
1.7.2 安全防护日志查询……1-42
1.7.3 病毒防护日志……1-45
1.7.4 WEB 规则防护日志……1-48
1.7.5 WEB 高级防护日志……1-50
1.7.6 行为模型日志……1-52
1.7.7 防暴力破解日志……1-55
1.7.8 弱密码防护日志……1-57
1.7.9 非法外联防护日志……1-59

1.8 终端日志 ····· 1-61
1.8.1 用户上下线日志 ····· 1-61
1.8.2 共享接入日志 ····· 1-63
1.8.3 移动终端日志 ····· 1-63
1.8.4 流量限额日志 ····· 1-64
1.9 日志导出 ····· 1-65
1.9.1 概述 ····· 1-65
1.9.2 系统日志导出 ····· 1-65
1.9.3 审计日志导出 ····· 1-66
1.10 日志典型配置举例 ····· 1-67
1.10.1 日志典型配置举例 ····· 1-67

1 日志

1.1 日志概述

日志是设备在运行过程中输出的信息，通过查看日志，管理员可以实时了解网络中各种业务的运行状态，掌握设备上各个功能模块的运行情况。

1.1.1 日志的类型

日志功能记录并输出各种日志信息，分别是系统日志、控制日志、审计日志、安全日志和终端日志。详细分类如表 1-1 所示。

表1-1 日志分类

日志分类	日志名称	描述
系统日志	系统日志	系统状态，如接口up、down事件
	操作日志	系统操作信息，如对系统进行的命令操作
控制日志	应用控制日志	应用控制策略产生的日志
	恶意URL日志	访问恶意网站产生的日志
审计日志	访问网站日志	访问网站产生的日志
	IM聊天软件日志	IM 即时通讯信息产生的日志，如QQ、MSN等
	社区日志	网络社区，微博、论坛等产生的日志
	搜索引擎日志	搜索引擎产生的日志
	邮件日志	通过SMTP、IMAP、POP3收发邮件的信息
	文件传输日志	FTP等文件传输产生的日志
	娱乐/股票日志	娱乐股票等信息
	协议审计日志	基础协议审计产生的日志
	其它应用日志	其它类型的应用日志，如P2P、网银等使用
安全日志	入侵日志	入侵检测策略产生的日志
	安全防护日志	网络层攻击防护产生的日志
	病毒防护日志	病毒防护策略产生的日志
	WEB防护日志	WEB防护策略产生的日志
	行为模型日志	行为模型策略产生的日志
	防暴力破解日志	防暴力破解策略产生的日志
	弱密码防护日志	弱密码防护策略产生的日志
	非法外联防护日志	非法外联防护策略产生的日志

日志分类	日志名称	描述
终端日志	共享接入日志	共享上网被惩罚阻断或限速的日志
	用户上下线日志	认证用户上下线的日志
	移动终端日志	移动终端接入的日志
	流量限额日志	用户流量限额策略产生的日志

1.1.2 日志的等级

日志信息是根据日志信息的严重程度区分的，根据严重程度不同，日志的严重等级可以分为 8 级，日志的级别如表 1-2 所示。

表1-2 日志的级别

级别	级别号	描述
紧急（emergencies）	0	系统不可用信息
告警（alerts）	1	需要立即处理的信息，如设备收到攻击等
严重（critical）	2	危机的信息，如硬件出错
错误（errors）	3	错误信息
警告（warnings）	4	报警信息
通知（notifications）	5	非错误信息，但需要特殊处理
信息（informational）	6	通知信息
调试(debug)	7	一般作为模块内部调试信息用

1.1.3 日志信息输出

日志信息可以输出到不同的目的地，支持以下几种日志信息输出目的地，用户可以根据自己的需要指定。具体的日志输出如表 1-3 所示。

表1-3 日志信息输出

目的地	描述
server	系统可以将日志发向syslog服务器
local	默认情况下，系统将日志记录在本地数据库

1.2 配置日志服务器

点击“系统管理 > 系统设定 > 日志设定 > 日志服务器”，进入日志服务器的配置页面，如图 1-1 所示。

图1-1 日志服务器配置

日志服务器的详细配置表如表 1-4 所示：

表1-4 日志服务器的详细配置

配置项	说明
启用	是否启用日志服务器，只有当启用的情况下，日志服务器的配置才会生效。
服务器1IP地址	第一台日志服务器的IP地址，支持IPv4及IPv6地址。
服务器1端口	第一台日志服务器的端口号
服务器2IP地址	第二台日志服务器的IP地址，支持IPv4及IPv6地址。
服务器3端口	第二台日志服务器的端口号
服务器3IP地址	第三台日志服务器的IP地址，支持IPv4及IPv6地址。
服务器3端口	第三台日志服务器的端口号
蝶式交换算法	发送给日志服务器的内容是否通过蝶式交换算法进行传输，默认为不勾选。
源IP地址	日志的源IP地址

说明

- 日志加密是为了防止在传输过程中泄露信息，和外置数据中心配合使用，发送给标准的日志服务器时不要启用日志加密。
- 如果没有特殊需求，不要配置日志的源 IP，让系统自动选择，在配置有 VPN 的情况的下，如果想让日志通过 VPN 隧道发送出去，可以指定源接口 IP 为 tunnel 接口的 IP 地址。

1.3 配置日志过滤

日志过滤的功能是对已经产生的日志进行过滤：

- 已经产生的日志是否记录在本地。
- 哪种级别以上的日志，发送给远端的日志服务器。

点击“系统管理 > 系统设定 > 日志设定 > 日志过滤”，进入日志过滤的配置页面，如图 1-2 所示：

图1-2 日志过滤配置

日志过滤的详细配置如所示：

表1-5 日志过滤详细配置

配置项	说明
探针日志	配置是否发送探针格式日志： • 不开启表示 syslog 日志按照非探针格式发送到日志服务器 • 开启表示 syslog 日志按照探针预定义格式发送到日志服务器 缺省情况下，默认关闭探针日志，以非探针日志格式发送到日志服务器。
本地日志	配置是否记录本地日志
Server日志	配置日志是否发送到日志服务器 • 不发送表示不发送到日志服务器 • 发送，发送指定级别的日志到日志服务器，全部级别发送所有的日志到日志服务器 缺省情况下，本地不记录会话日志和NAT，其它类型的日志本地会记录，对发送到远端的日志不做过滤

1.4 系统日志查询

1.4.1 系统日志查询

系统日志记录系统的状态信息，比如接口的 up/ down、管理的登录、退出等。点击“数据中心 > 日志中心 > 系统日志”，进入系统日志的查询界面，如图 1-3 所示。

图1-3 系统日志查询页面

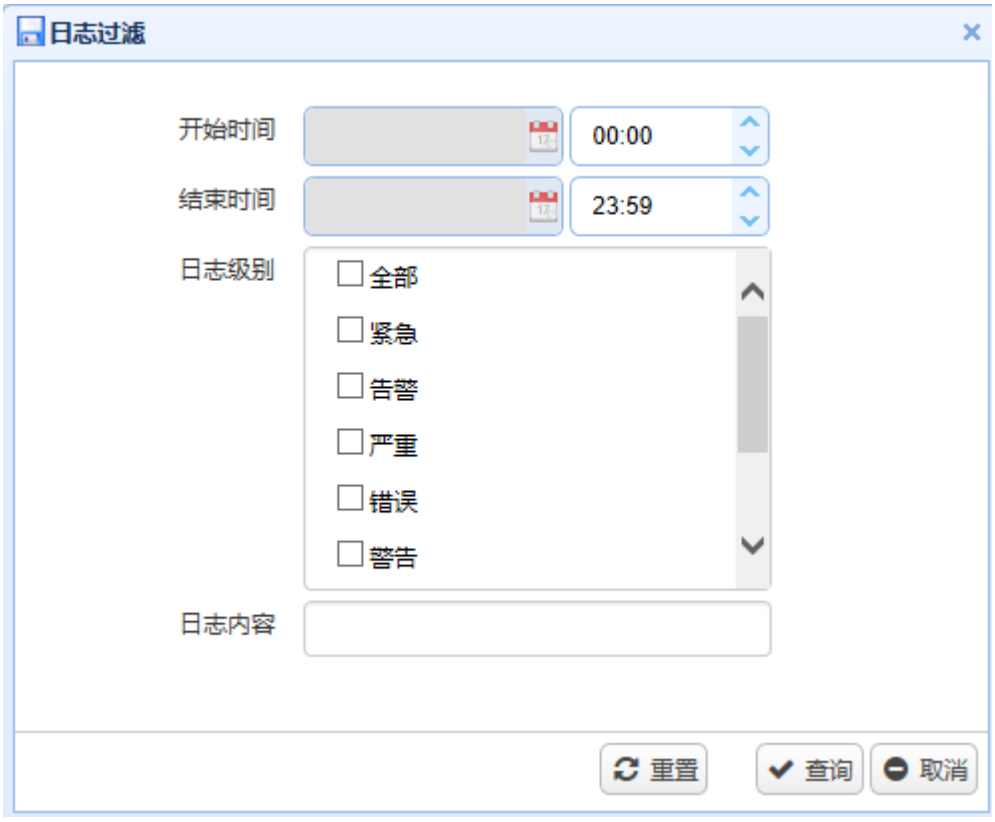
系统日志的显示信息如表 1-6 所示：

表1-6 系统日志显示信息描述表

配置项	说明
时间	日志产生的时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 严重 • 警告
日志内容	系统日志的内容

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-4 所示。

图1-4 系统日志查询界面



系统日志查询的详细信息如表 1-7 所示。

表1-7 系统日志查询详细信息

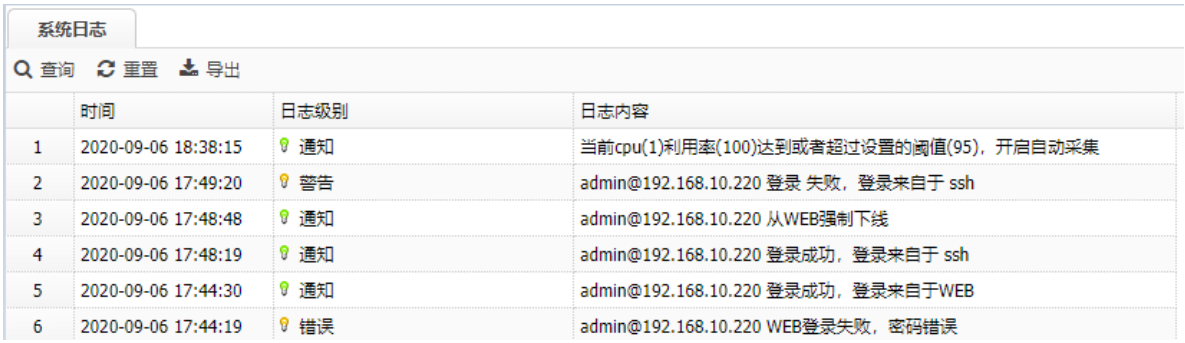
配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间

配置项	说明
日志级别	选择一个或者多个级别的日志 • 信息 • 通知 • 警告 • 严重 • 警告
日志内容	系统日志的内容，支持模糊查询

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可导出所有系统日志。

图1-5 导出系统日志



1.4.2 操作日志查询

操作日志记录着管理员对系统的操作，点击“数据中心 > 日志中心 > 操作日志”，进入操作日志的查询界面，如图 1-6 所示。

图1-6 操作日志查询界面

操作日志的显示信息如表 1-8 所示：

表1-8 操作日志显示信息描述表

配置项	说明
时间	日志产生的时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 严重 • 警告
操作管理员	进行操作的管理员的名称
操作员IP	执行操作的管理员的IP，如果通过console操作设备，管理员IP是127.0.0.1
详细信息	管理员名称，操作的方式，操作的结果是成功还是失败
操作内容	管理员执行操作的内容

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-7 所示。

图1-7 操作日志查询界面

操作日志查询的详细信息如表 1-9 所示。

表1-9 操作日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
操作管理员	操作管理员的名称，支持模糊查询
操作员IP	操作员的IP地址
日志的级别	选择一个或者多个级别的日志 • 信息 • 通知 • 警告 • 严重 • 警告
日志内容	操作日志的内容，支持模糊查询

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以下载所有操作日志到本地。

图1-8 导出操作日志

1.5 控制日志查询

1.5.1 应用控制日志查询

应用控制日志记录着应用控制策略产生的日志。点击“数据中心 > 日志中心 > 控制日志 > 应用控制日志”，进入应用控制日志的查询界面，如图 1-9 所示。

图1-9 应用控制日志查询页面

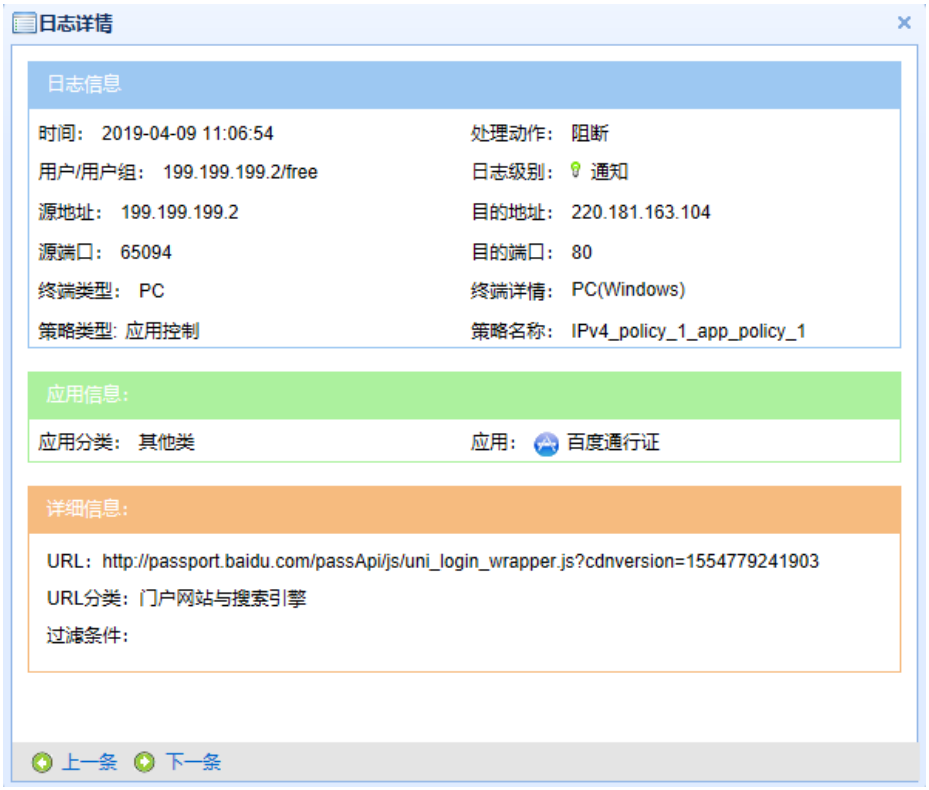
应用控制日志的显示信息如表 1-10 所示：

表1-10 应用控制日志显示信息描述表

配置项	说明
用户	产生日志的用户
用户mac	产生日志的用户mac
应用分类	应用的类别
应用	应用的名称
策略类型	控制策略的类型：应用控制、URL控制、搜索控制、邮件控制、虚拟账户控制等。
处理动作	设备的处理动作，允许或者阻断
终端	使用的终端类型，比如PC、iPhone、iPad等
级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 错误 • 严重 • 警告 • 紧急 • 调试
时间	日志产生的时间

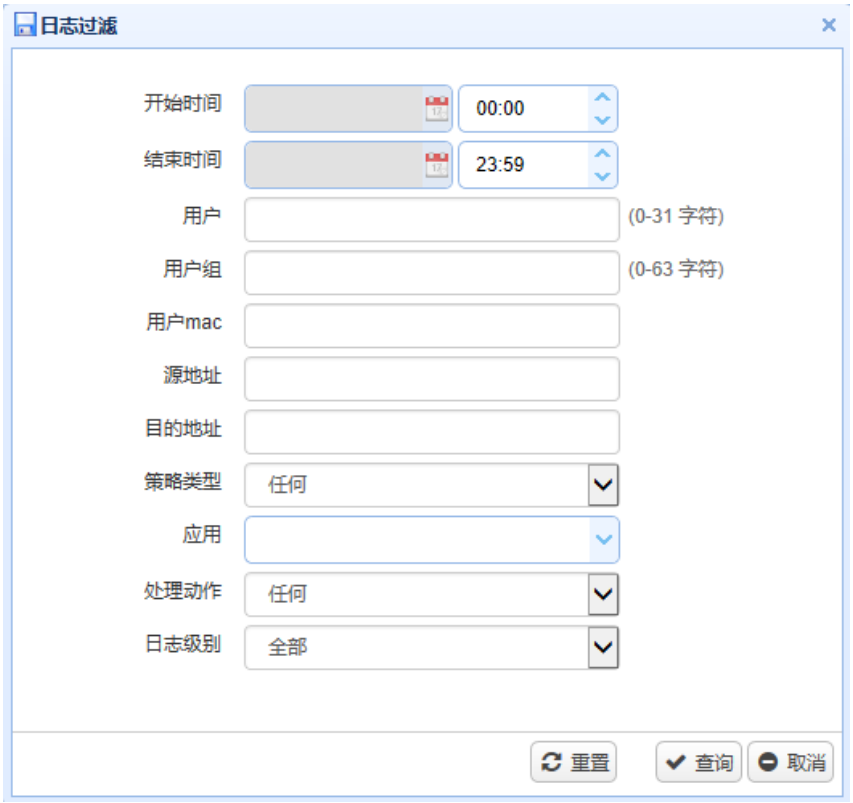
点击对应应用控制日志的<详细>按钮，可以查看日志的详细信息，如图 1-10 所示。在日志详情的下方，点击<上一条>、<下一条>可以切换到上一条或下一条日志的详情界面。

图1-10 应用控制日志详情



点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-11 所示。

图1-11 应用控制日志查询界面



应用控制日志查询的详细信息如表 1-11 所示。

表1-11 应用控制日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
用户	日志的用户
用户组	日志的用户所属的用户组
用户mac	日志的用户mac信息
源地址	应用控制日志的源地址
目的地址	应用控制日志的目的地址
策略类型	控制策略的类型
应用	应用的名称
处理动作	设备的处理动作，允许或者阻断
日志级别	应用控制日志的级别

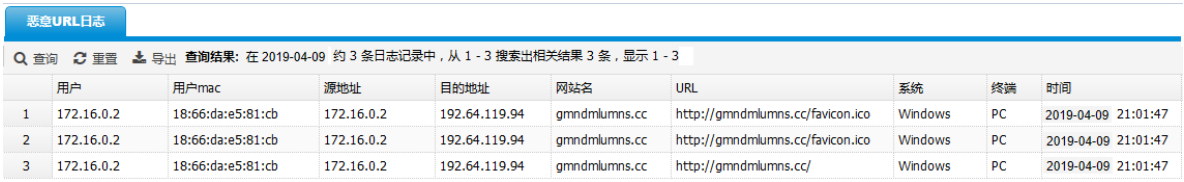
点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以根据设定的日志开始、结束时间范围，导出相关的应用控制日志到本地。

1.5.2 恶意 URL 日志

恶意 URL 日志记录着访问恶意网站的信息，点击“数据中心 > 日志中心 > 控制日志 > 恶意 URL 日志”，进入恶意 URL 的查询界面，如图 1-12 所示。

图1-12 恶意 URL 日志查询页面



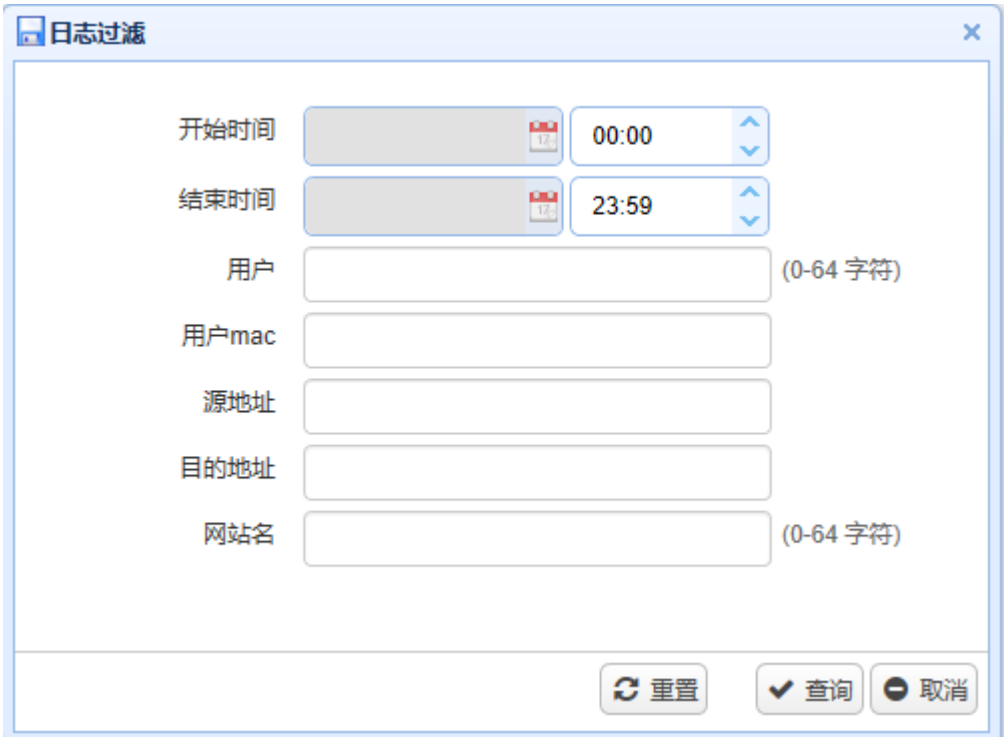
访问网站日志的显示信息如表 1-12 所示：

表1-12 恶意 URL 日志显示信息描述表

配置项	说明
用户	产生日志的用户
用户mac	访问网站的源mac地址
源地址	访问网站的源IP地址
目的地址	访问网站的目的IP地址
网站名	访问网站的域名
URL	访问网站的URL
系统	访问网站的操作系统及平台信息
终端	访问网站的终端类型，比如iPhone、iPad等
时间	访问网站的时间

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-13 示。

图1-13 恶意 URL 日志查询界面



恶意 URL 日志查询的详细信息如表 1-13 所示。

表1-13 恶意 URL 日志查询详细信息

配置项	说明
开始时间	开始记录的时间点
结束时间	结束记录的时间点
用户	用户名称
用户mac	用户访问网站的mac信息
源地址	访问网站日志的源地址
目的地址	访问网站日志的目的地址
网站名	访问网站的域名，支持模糊搜索

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮之后，可以根据设定的日志开始、结束时间范围，导出相关的访问网站日志到本地。

1.6 审计日志查询

1.6.1 访问网站日志

访问网站日志记录着所有访问网站的信息，点击“数据中心 > 日志中心 > 审计日志 > 访问网站日志”，进入访问网站日志的查询界面，如图 1-14 所示。

图1-14 访问网站日志查询页面

访问网站日志的显示信息如表 1-14 所示：

表1-14 访问网站日志显示信息描述表

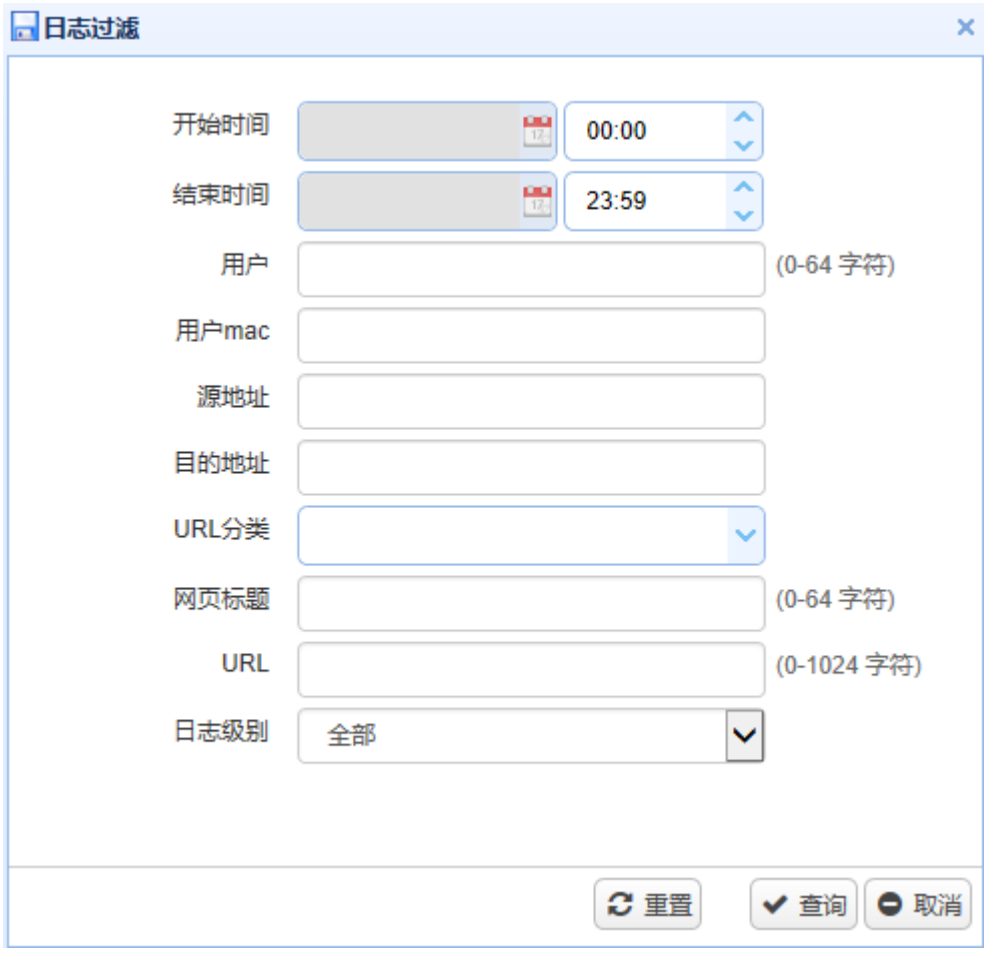
配置项	说明
用户	产生日志的用户
用户mac	产生日志的用户mac信息
URL分类	访问网站的URL类别
网页标题	访问网站的标题
URL	URL地址链接
级别	访问网站日志的级别
时间	访问网站的时间

点击对应访问网站日志的<详细>按钮，可以查看日志的详细信息，如图 1-15 所示。在日志详情的下方，点击<上一条>、<下一条>可以切换到上一条或下一条日志的详情界面。

图1-15 访问网站日志详情

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-16 所示。

图1-16 访问网站日志查询界面



访问网站日志查询的详细信息如表 1-15 所示。

表1-15 访问网站日志查询详细信息

配置项	说明
开始时间	开始记录的时间点
结束时间	结束记录的时间点
用户	用户名称
用户mac	访问网站日志的源mac
源地址	访问网站日志的源地址
目的地址	访问网站日志的目的地址
URL分类	访问网站日志的URL分类
处理动作	访问网站人处理动作，可选的值有是：阻断、放行或者任何
级别	日志的级别

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮之后，可以根据设定的日志开始、结束时间范围，导出相关的日志到本地。

1.6.2 IM 聊天软件日志

IM 聊天软件日志记录着 IM 聊天软件使用相关的信息，点击“数据中心 > 日志中心 > 审计日志 > IM 聊天软件日志”，进入 IM 聊天软件日志的查询界面，如图 1-17 所示。

图1-17 IM 聊天软件日志查询页面

IM 聊天软件日志的显示信息如表 1-16 所示：

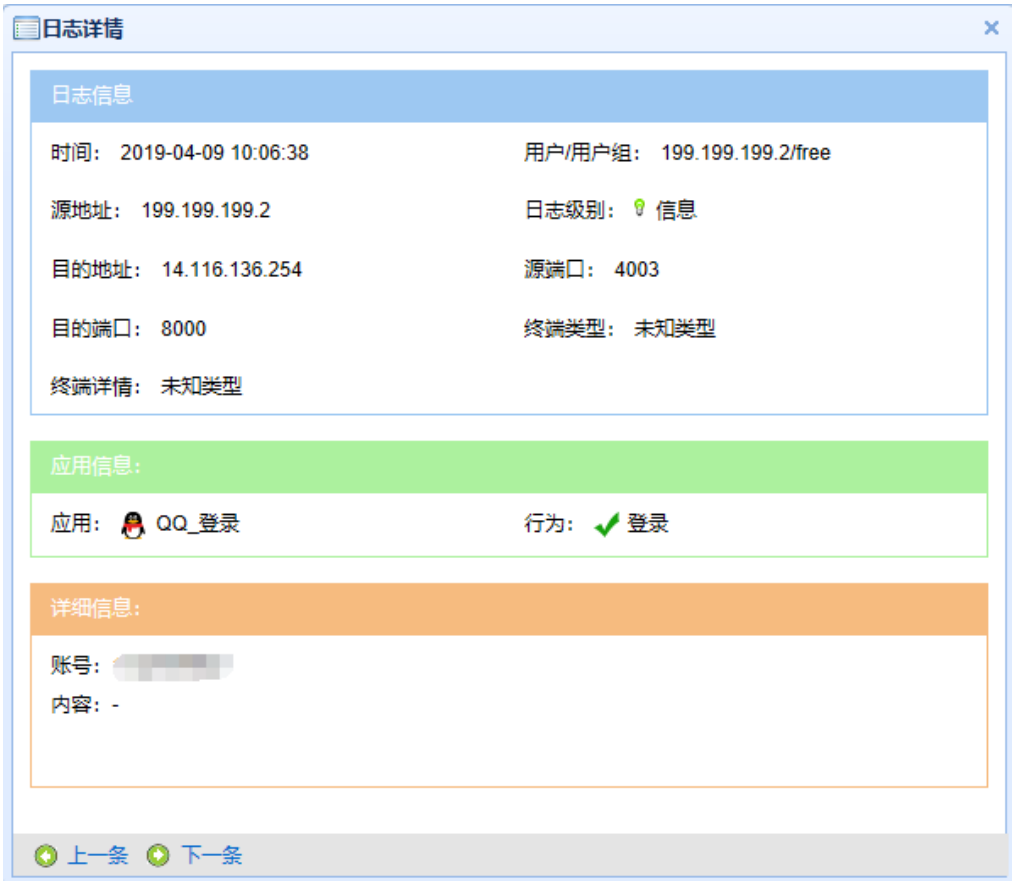
表1-16 IM 聊天软件日志显示信息描述表

配置项	说明
用户	产生日志的用户
用户mac	产生日志的用户mac
应用	应用的名称
行为	应用的行为，比如登录、注销、收消息、发消息、发文件等
帐号	聊天软件的帐号，如果聊天软件为微信时，账号显示的为微信用户的uin，不是用户登录微信的账号（uin即user information，是微信用户的唯一识别码）。
系统	用户使用的操作系统
平台	用户使用的平台，比如windows、android、ios等
终端	使用的终端类型，比如iPhone、iPad等
处理动作	设备的处理动作，允许或者阻断
级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 错误 • 严重 • 警告 • 紧急 • 调试

配置项	说明
时间	日志产生的时间

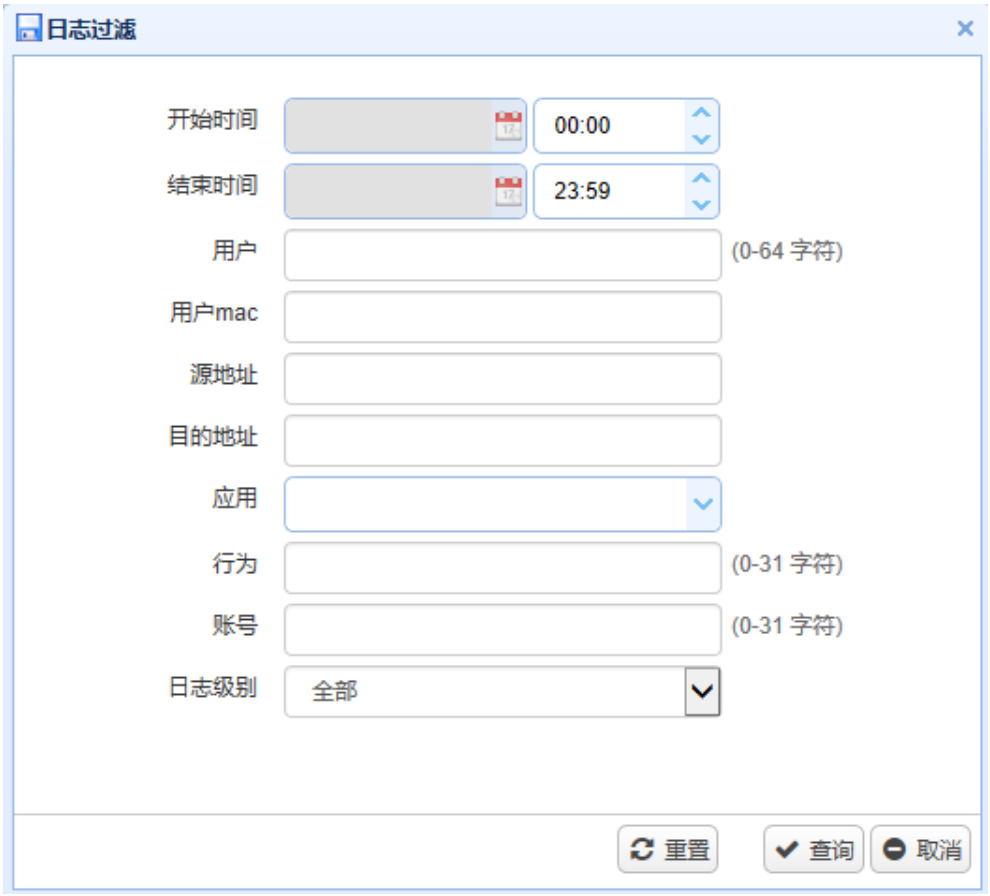
点击对应 IM 聊天日志的<详细>按钮，可以查看日志的详细信息，如图 1-18 所示。在日志详情的下方，点击<上一条>、<下一条>可以切换到上一条或下一条日志的详情界面。

图1-18 IM 聊天软件日志详情



点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-19 所示。

图1-19 IM 聊天软件日志日志查询界面



IM 聊天软件日志查询的详细信息如表 1-17 所示。

表1-17 IM 聊天软件日志查询详细信息

配置项	说明
开始时间	开始记录的时间点
结束时间	结束记录的时间点
用户	用户名称
用户mac	用户mac信息
源地址	访问网站日志的源地址
目的地址	访问网站日志的目的地址
应用分类	应用的分类名称
应用	应用的名称
行为	应用的行为
帐号	应用的帐号
内容	聊天软件的内容

配置项	说明
处理动作	日志的动作，放行或者阻断
日志级别	日志的级别

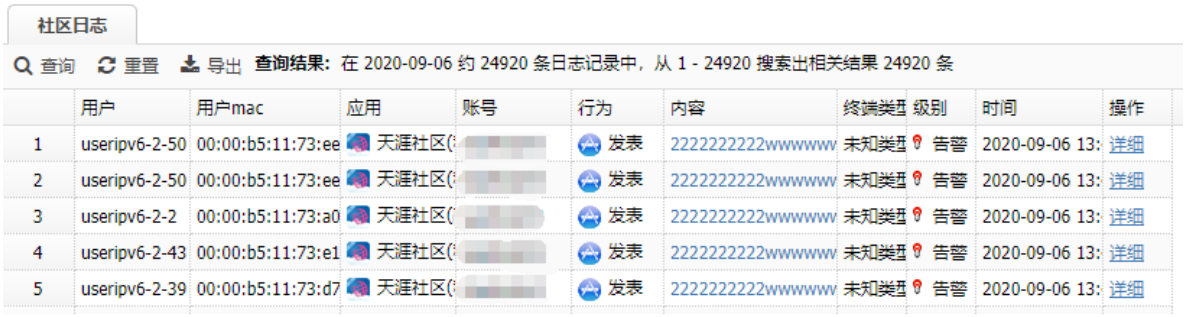
点击<查询>按钮之后，可以显示出符合设置的条件的日志。

点击<导出>按钮之后，可以根据设定的日志开始、结束时间范围，导出相关的日志到本地。

1.6.3 社区日志

社区日志记录着微博、BBS、博客等网络社区相关的信息，点击“数据中心 > 日志中心 > 审计日志 > 社区日志”，进入社区日志的查询界面，如图 1-20 所示。

图1-20 社区日志查询页面



社区日志的显示信息如表 1-18 所示：

表1-18 社区日志显示信息描述表

配置项	说明
用户	产生日志的用户
用户mac	产生日志的用户mac信息
应用	应用的名称
行为	应用的行为，登录、发表、注销等
帐号	社区的帐号
内容	社区的内容
系统	用户使用的操作系统以及使用平台
终端	使用的终端类型，比如iPhone、iPad等
级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 错误 • 严重

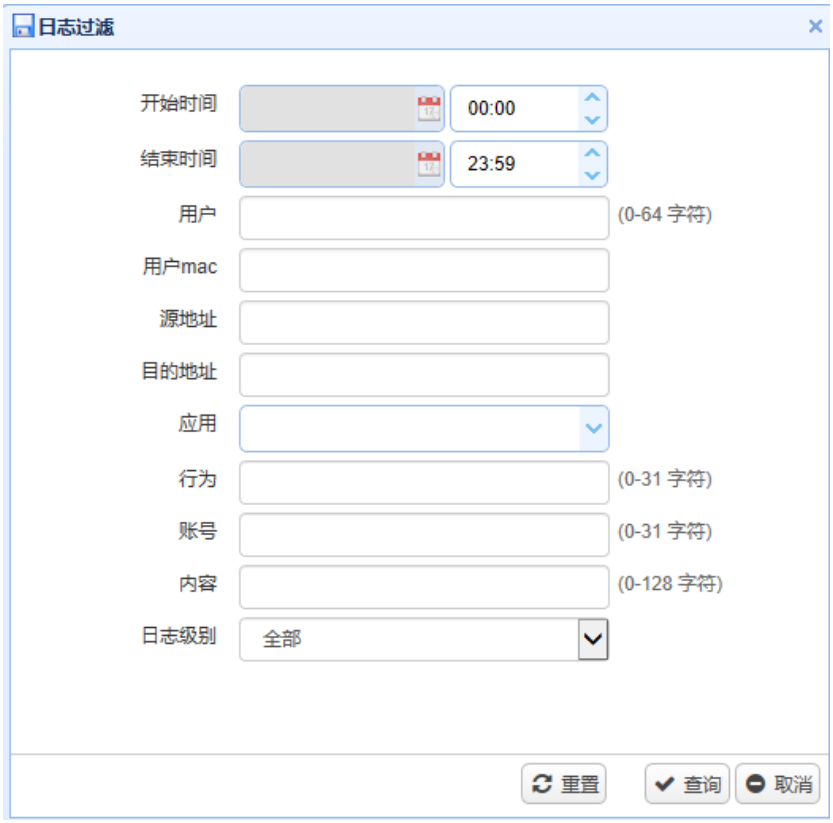
配置项	说明
	• 警告 • 紧急 • 调试
时间	日志产生的时间

点击对应社区日志的<详细>按钮，可以查看日志的详细信息，如图 1-21 所示。在日志详情的下方，点击<上一条>、<下一条>可以切换到上一条或下一条日志的详情界面。

图1-21 社区日志详情

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-22 所示。

图1-22 社区日志查询界面



社区日志查询的详细信息如表 1-19 所示。

表1-19 社区日志查询详细信息

配置项	说明
开始时间	开始记录的时间点
结束时间	结束记录的时间点
用户	用户名称
用户mac	用户mac信息
源地址	访问网站日志的源地址
目的地址	访问网站日志的目的地址
应用分类	应用的分类名称
应用	应用的名称
行为	社区的行为
帐号	社区的帐号，支持模糊搜索
内容	社区的内容
日志级别	日志的级别
处理动作	日志的动作，放行或者阻断

点击<导出>按钮之后，可以根据设定的日志开始、结束时间范围，导出相关的日志到本地。

1.6.4 搜索引擎日志

搜索引擎日志记录着搜索引擎使用的信息，点击“数据中心 > 日志中心 > 审计日志 > 搜索引擎日志”，进入搜索引擎日志的查询界面，如图 1-23 所示。

图1-23 搜索引擎日志查询页面

搜索引擎日志的显示信息如表 1-20 所示：

表1-20 搜索引擎日志显示信息描述表

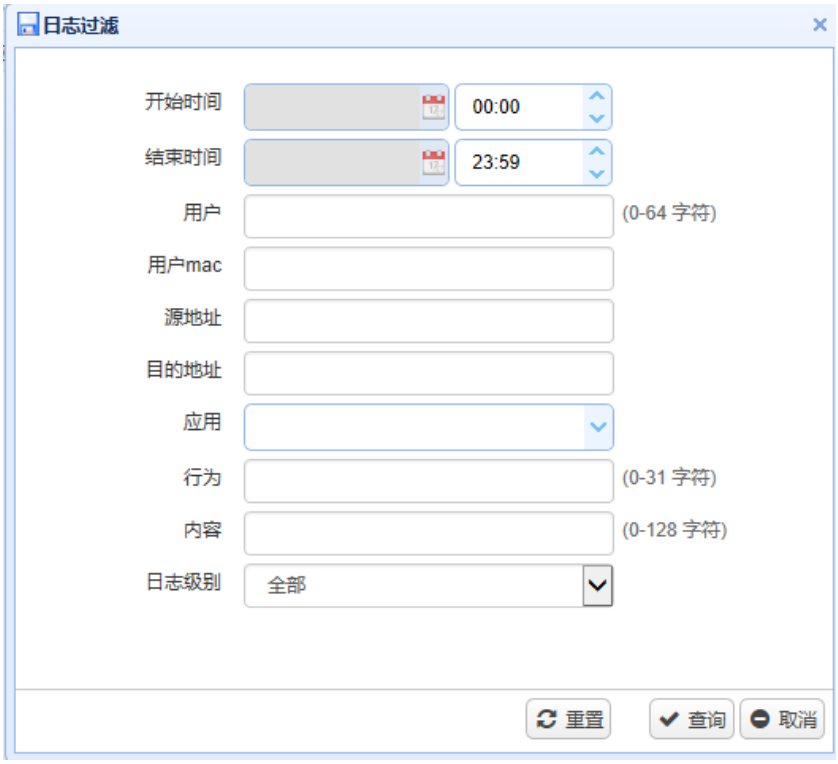
配置项	说明
用户	日志的用户
用户mac	日志的用户mac信息
应用	应用的名称
行为	应用的行为，搜索等
内容	搜索引擎的内容
系统	用户使用的操作系统以及平台信息
终端	使用的终端类型，比如iPhone、iPad等
级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 错误 • 严重 • 警告 • 紧急 • 调试
时间	日志产生的时间

点击对应日志的<详细>按钮，可以查看日志的详细信息，如图 1-24 所示。在日志详情的下方，点击<上一条>、<下一条>可以切换到上一条或下一条日志的详情界面。

图1-24 搜索引擎日志详情

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-25 所示。

图1-25 搜索引擎日志查询界面



搜索引擎日志查询的详细信息如表 1-21 所示。

表1-21 搜索引擎日志查询详细信息

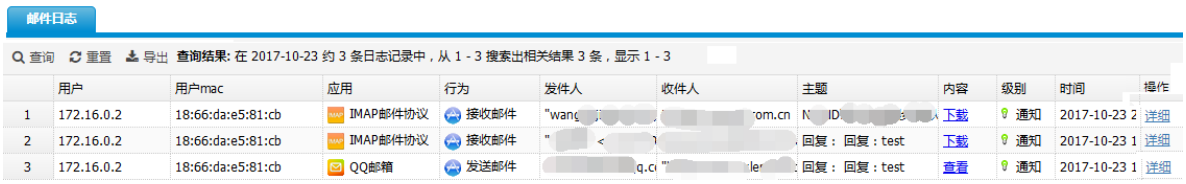
配置项	说明
开始时间	开始记录的时间点
结束时间	结束记录的时间点
用户	用户名称
源地址	访问网站日志的源地址
目的地址	访问网站日志的目的地址
应用分类	应用的分类名称
应用	应用的名称
行为	搜索引擎的行为
内容	搜索引擎的内容
处理动作	日志的动作，放行或者阻断
日志级别	日志的级别

点击<导出>按钮之后，可以根据设定的日志开始、结束时间范围，导出相关的日志到本地。

1.6.5 邮件日志

邮件日志记录通过 SMTP、IMAP、POP3 收发邮件的信息，点击“数据中心 > 日志中心 > 审计日志 > 邮件日志”，进入邮件日志的查询界面，如图 1-26 所示。

图1-26 邮件日志查询页面



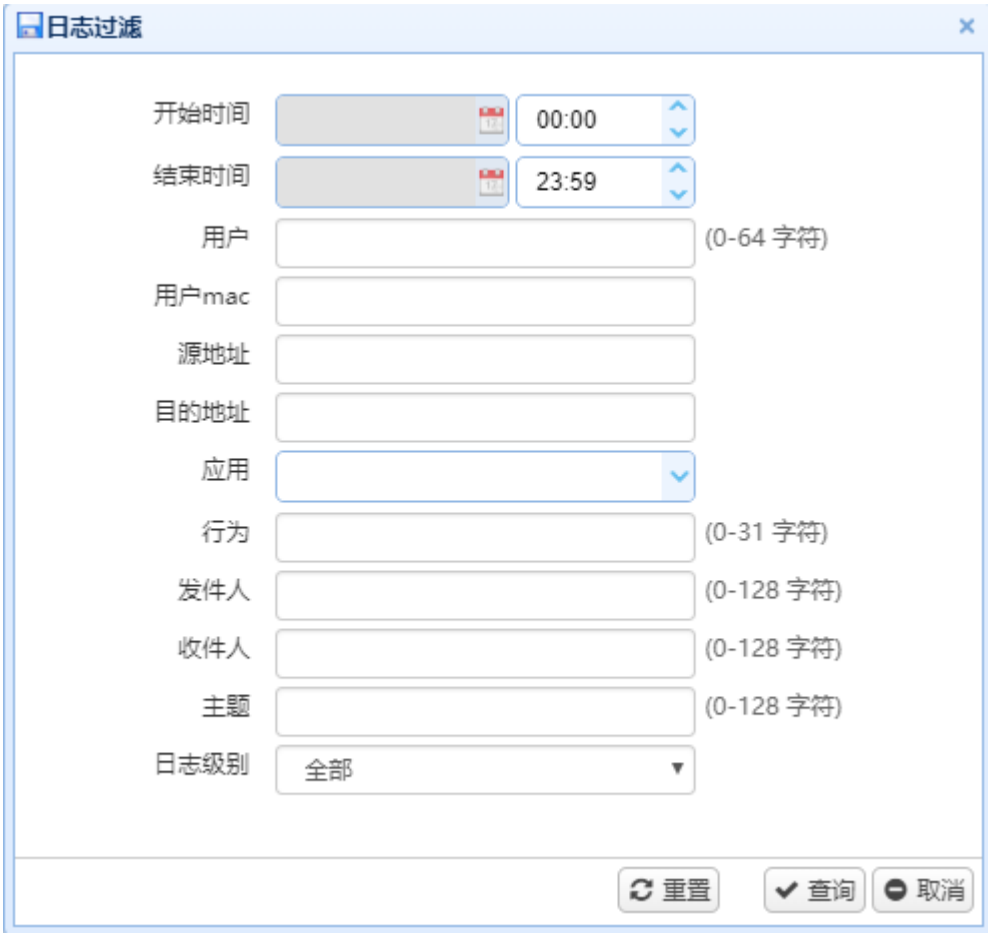
邮件日志的显示信息如表 1-22 所示：

表1-22 邮件日志显示信息描述表

配置项	说明
用户	日志的用户
用户mac	用户的mac信息
应用	应用的名称
发件人	邮件的发件人
收件人	邮件的接收人
主题	邮件主题
行为	邮件的行为
内容	邮件内容
级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 错误 • 严重 • 警告 • 紧急 • 调试
时间	日志产生的时间

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-27 所示。

图1-27 邮件日志查询界面



邮件日志查询的详细信息如表 1-23 所示。

表1-23 邮件日志查询详细信息

配置项	说明
开始时间	开始记录的时间点
结束时间	结束记录的时间点
用户	用户名称
源地址	访问网站日志的源地址
目的地址	访问网站日志的目的地址
应用	应用的名称
行为	邮件的行为
发件人	邮件的发送者，支持模糊查询
收件人	邮件的接收者，支持模糊查询
主题	邮件的主题，支持模糊查询
日志级别	日志的级别

点击<导出>按钮之后，可以根据设定的日志开始、结束时间范围，导出相关的日志到本地。

图1-28 导出邮件日志

1.6.6 文件传输日志

命令日志记录网盘和 FTP、telnet 使用的信息，点击“数据中心 > 日志中心 > 审计日志 > 文件传输日志”，进入文件传输日志的查询界面，如图 1-29 所示。

图1-29 文件传输日志查询页面

文件传输日志的显示信息如表 1-24 所示：

表1-24 文件传输日志显示信息描述表

配置项	说明
用户	日志的用户
用户mac	日志的用户mac信息
应用	应用的名称
行为	应用的行为
帐号	应用的帐号
行为	文件传输过程中的行为，如登录、下载文件等
文件	传输的文件名
系统	用户使用的操作系统
终端	使用的终端类型，比如iPhone、iPad等
级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告

配置项	说明
	• 错误 • 严重 • 警告 • 紧急 • 调试
时间	日志产生的时间
操作	点击这些链接，可以查看日志详情

点击对应日志的<详细>按钮，可以查看日志的详细信息，如图 1-30 所示。在日志详情的下方，点击<上一条>、<下一条>可以切换到上一条或下一条日志的详情界面。

图1-30 文件传输日志详情

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-31 所示。

图1-31 文件传输日志查询界面

命令日志查询的详细信息如表 1-25 所示。

表1-25 命令日志查询详细信息

配置项	说明
开始时间	开始记录的时间点
结束时间	结束记录的时间点
用户	用户名称
源地址	访问网站日志的源地址
目的地址	访问网站日志的目的地址
应用	应用的名称
行为	命令的行为
帐号	应用的帐号，支持模糊查询
文件	传输的文件名，支持模糊查询
日志级别	日志的级别

点击<导出>按钮之后，可以根据设定的日志开始、结束时间范围，导出相关的日志到本地。

1.6.7 娱乐/股票日志

娱乐/股票日志记录用户上网娱乐信息，如看视频、玩在线游戏、听音乐、炒股等行为，点击“数据中心 > 日志中心 > 审计日志 > 娱乐/股票日志”，进入娱乐/股票日志的查询界面，如图 1-32 所示。

图1-32 娱乐/股票日志查询页面

娱乐/股票应用日志的显示信息如表 1-26 所示：

表1-26 娱乐/股票日志显示信息描述表

配置项	说明
用户	日志的用户
用户mac	日志的用户mac信息
应用	应用的名称
行为	应用的行为
系统	用户使用的操作系统
终端	使用的终端类型，比如iPhone、iPad等
级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 错误 • 严重 • 警告 • 紧急 • 调试
时间	日志产生的时间
操作	点击这些链接，可以查看日志详情

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-33 所示。

图1-33 娱乐/股票日志查询界面

娱乐/股票日志查询的详细信息如表 1-27 所示。

表1-27 娱乐/股票日志查询详细信息

配置项	说明
开始时间	开始记录的时间点
结束时间	结束记录的时间点
用户	用户名称
用户mac	用户名称mac
源地址	访问网站日志的源地址
目的地址	访问网站日志的目的地址
应用	应用的名称
行为	其它应用的行为
帐号	应用的帐号，支持模糊查询
内容	应用的内容
日志级别	日志的级别

点击<导出>按钮之后，可以根据设定的日志开始、结束时间范围，导出相关的日志到本地。

1.6.8 协议审计日志

协议审计日志记录基础网络协议的信息，如账号、文件名、命令操作等行为，点击“数据中心 > 日志中心 > 审计日志 >协议审计日志”，进入娱乐/股票日志的查询界面，如下图所示。

图1-34 娱乐/股票日志查询页面

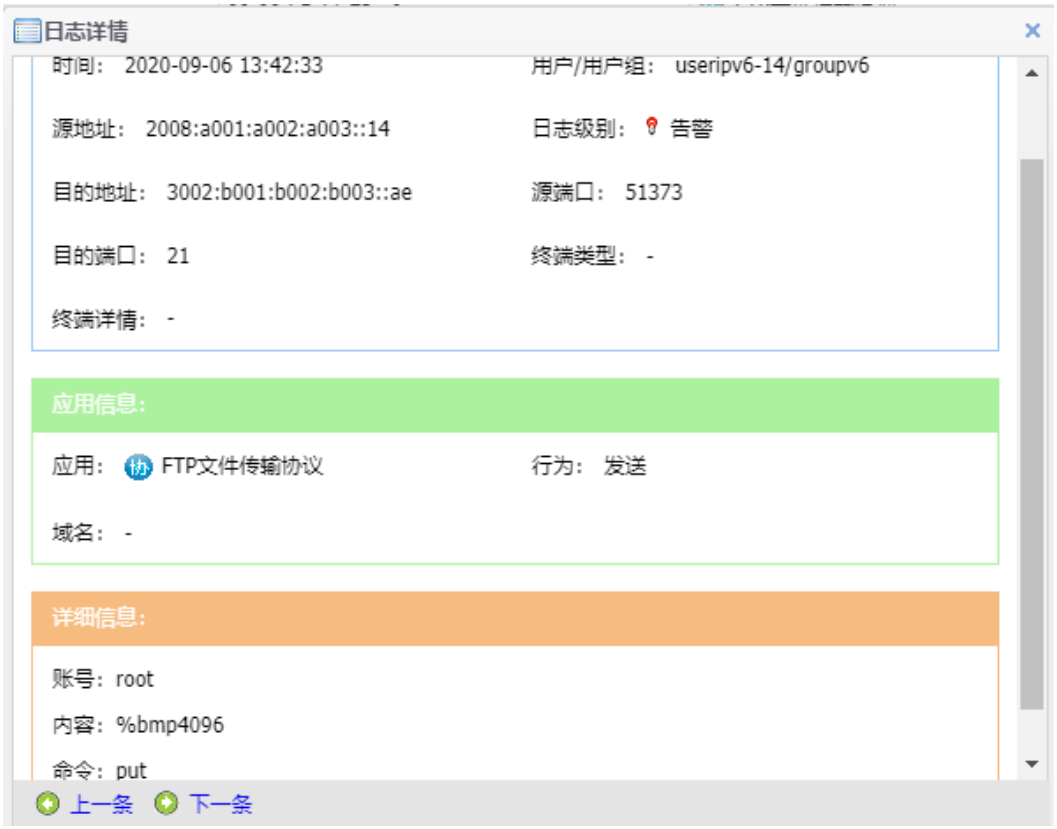
协议审计日志的显示信息如下表所示：

表1-28 娱乐/股票日志显示信息描述表

配置项	说明
用户	日志的用户
用户mac	日志的用户mac信息
应用	应用的名称
账号	应用的账号
级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 错误 • 严重 • 警告 • 紧急 • 调试
时间	日志产生的时间
操作	点击这些链接，可以查看日志详情

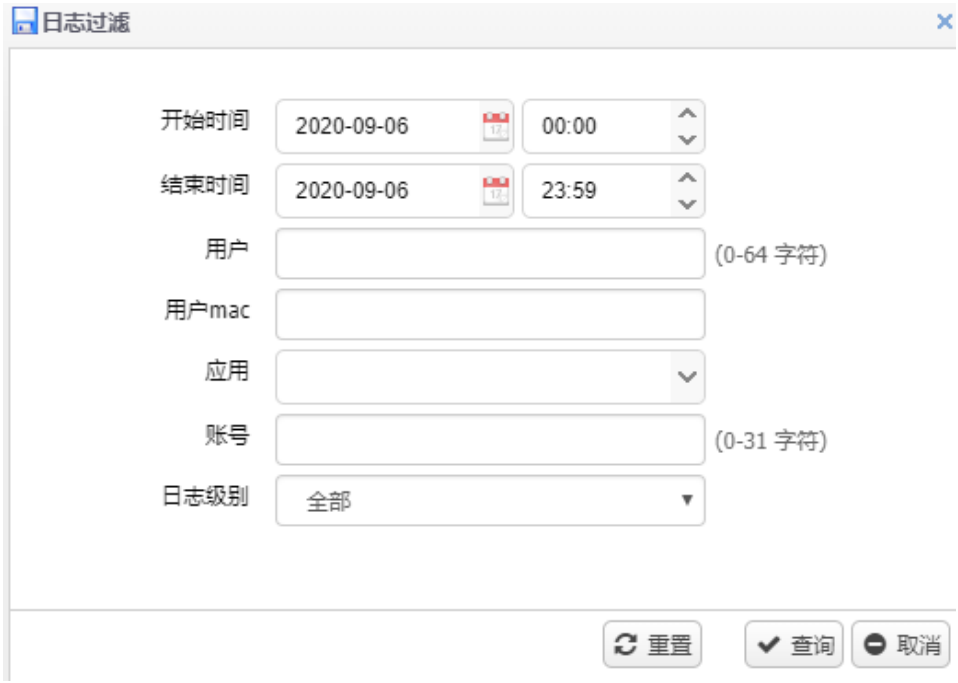
点击对应日志的<详细>按钮，可以查看日志的详细信息，在日志详情的下方，点击<上一条>、<下一条>可以切换到上一条或下一条日志的详情界面。

图1-35 协议审计日志详情



点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如下图所示。

图1-36 协议审计日志查询界面



娱乐/股票日志查询的详细信息如表 1-27 所示。

表1-29 娱乐/股票日志查询详细信息

配置项	说明
开始时间	开始记录的时间点
结束时间	结束记录的时间点
用户	用户名称
用户mac	用户名称mac
应用	应用的名称
帐号	应用的帐号，支持模糊查询
日志级别	日志的级别

点击<导出>按钮之后，可以根据设定的日志开始、结束时间范围，导出相关的日志到本地。

1.6.9 其它应用日志

其它应用日志是除了聊天软件、社区、邮件、搜索引擎、命令之外的应用审计日志，点击“数据中心 > 日志中心 > 审计日志 > 其它应用日志”，进入其它应用日志的查询界面，如图 1-37 所示。

图1-37 其它应用日志查询页面

其它应用日志的显示信息如表 1-30 所示：

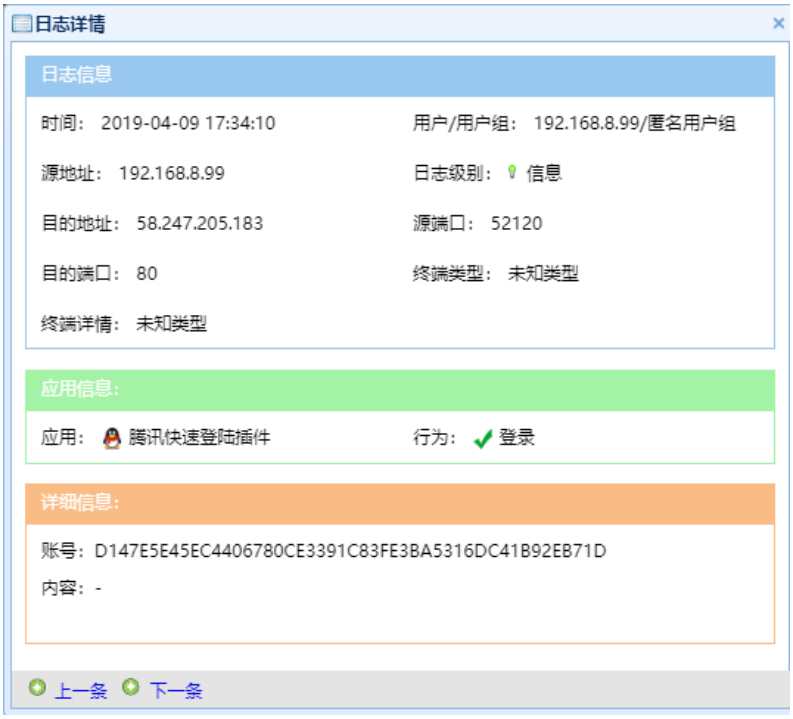
表1-30 其它应用日志显示信息描述表

配置项	说明
用户	日志的用户
用户mac	日志的用户mac信息
应用	应用的名称
行为	应用的行为
终端	使用的终端类型，比如iPhone、iPad等
级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知

配置项	说明
	• 警告 • 错误 • 严重 • 警告 • 紧急 • 调试
时间	日志产生的时间
操作	点击这些链接，可以查看日志详情

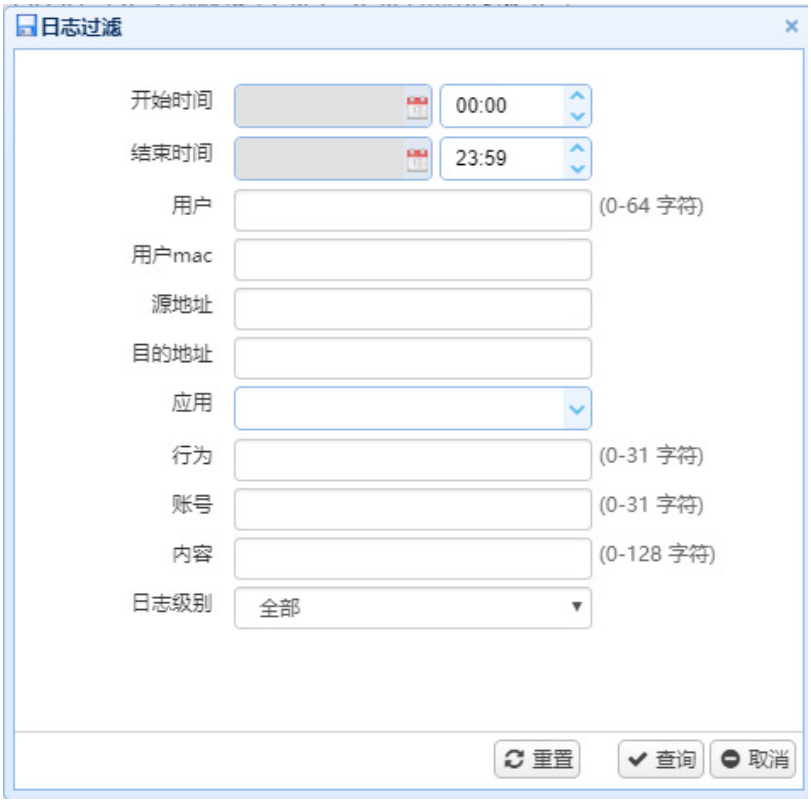
点击对应日志的<详细>按钮，可以查看日志的详细信息，如图 1-21 所示。在日志详情的下方，点击<上一条>、<下一条>可以切换到上一条或下一条日志的详情界面。

图1-38 其它应用日志详情



点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-39 所示。

图1-39 其它应用日志查询界面



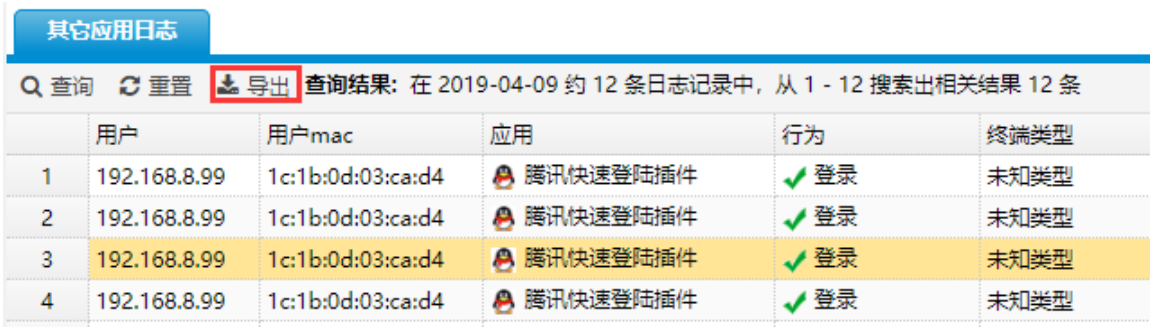
其它应用日志查询的详细信息如表 1-31 所示。

表1-31 其它应用日志查询详细信息

配置项	说明
开始时间	开始记录的时间点
结束时间	结束记录的时间点
用户	用户名称
用户mac	用户mac信息
源地址	访问网站日志的源地址
目的地址	访问网站日志的目的地址
应用	应用的名称
行为	其它应用的行为
帐号	应用的帐号，支持模糊查询
内容	应用的内容，支持模糊查询
日志级别	日志的级别

点击<导出>按钮之后，可以根据设定的日志开始、结束时间范围，导出相关的日志到本地。

图1-40 导出其它应用日志



1.7 安全日志查询

1.7.1 入侵日志

1. 入侵日志查询

入侵日志记录着针对网络的 IPS 攻击的日志。点击“数据中心 > 日志中心 > 安全日志 > 入侵日志”，进入入侵日志的查询界面，如图 1-41 所示。

图1-41 入侵日志查询页面

入侵日志的显示信息如表 1-32 所示：

表1-32 入侵检查日志显示信息描述表

配置项	说明
时间	日志产生的时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 告警 • 警告 • 通知 • 信息
用户名称	用户名称
源地址	攻击的源IP地址及端口
归属地	源地址所属归属地

配置项	说明
目的地址	攻击的目的IP地址及端口
事件名称	IPS事件的名称
事件类型	IPS事件的类型
行为	设备的处理行为

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-42 所示。

图1-42 入侵检测日志查询界面

入侵日志查询的详细信息如表 1-33 所示。

表1-33 入侵日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
日志的级别	选择一个或者多个级别的日志

配置项	说明
	• 告警 • 警告 • 通知 • 信息
事件名称	IPS事件的名称
用户名称	用户名称
事件类型	IPS事件的类型
行为	设备的处理行为
源地址	攻击的源IP地址及端口
目的地址	攻击的目的IP地址及端口

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以导出所有入侵日志到本地。

2. 告警规则

告警规则主要针对记录 IPS 攻击的日志按照匹配条件进行 syslog 或者邮件告警。点击“数据中心 > 日志中心 > 安全日志 > 入侵日志>告警规则”，点击“新建”按钮进入告警规则的配置界面，如图1-43 所示。

图1-43 告警规则页面

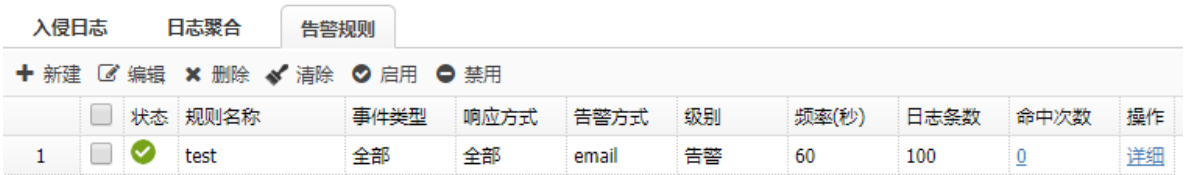


表1-34 入侵检测告警规则界面详细说明

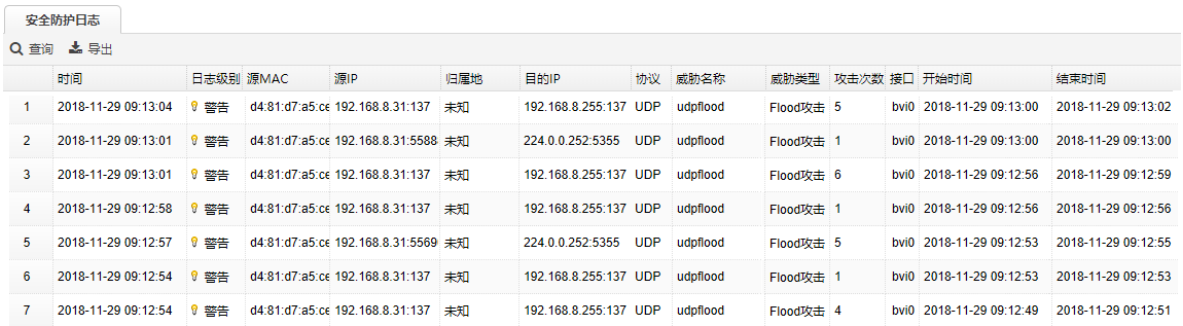
配置项	说明
新建	新建入侵检测告警规则
删除	删除入侵检测告警规则
清除	清除入侵检测告警规则命中次数统计及日志
启用	启用入侵检测告警规则
禁用	禁用入侵检测告警规则
状态	显示告警规则启用或禁用状态
规则名称	告警规则名称
事件类型	IPS事件类型
响应方式	IPS事件处理行为

配置项	说明
告警方式	支持syslog和邮件两种告警方式
级别	根据严重程度的不同，日志分为以下几个级别： 告警 警告 信息 通知
频率(秒)	告警检测的时间阈值
日志条数	告警检测的IPS日志条数阈值
命中次数	告警检测命中次数统计

1.7.2 安全防护日志查询

安全防护日志记录着针对网络层攻击的安全防护产生的日志。点击“数据中心 > 日志中心 > 安全日志 > 安全防护日志”，进入安全防护日志的查询界面，如图 1-44 所示。

图1-44 安全防护日志查询页面



安全防护日志的显示信息如表 1-35 所示：

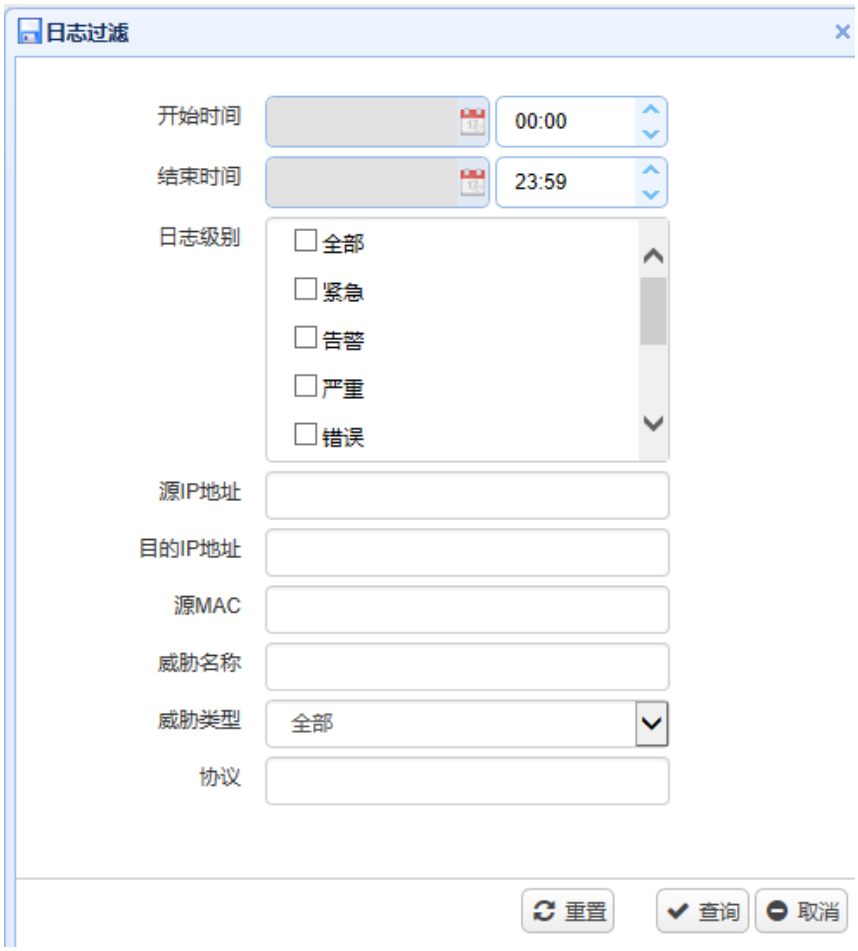
表1-35 安全防护日志显示信息描述表

配置项	说明
时间	日志产生的时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 严重 • 警告
源MAC	攻击报文的源MAC地址

配置项	说明
源IP	攻击的源IP地址及端口
目的IP	攻击的目的IP地址及端口
协议	攻击的协议类型
威胁名称	威胁的名称
威胁类型	威胁的类型。总共有4种类型： • 异常包攻击 • 扫描攻击 • Flood 攻击 • ARP 攻击
攻击次数	发生攻击的次数
接口	发生攻击的接口
开始时间	发生攻击的开始时间
结束时间	发生攻击的结束时间

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-45 所示。

图1-45 网络层攻击日志查询界面



安全防护日志查询的详细信息如表 1-36 所示。

表1-36 安全防护日志查询详细信息

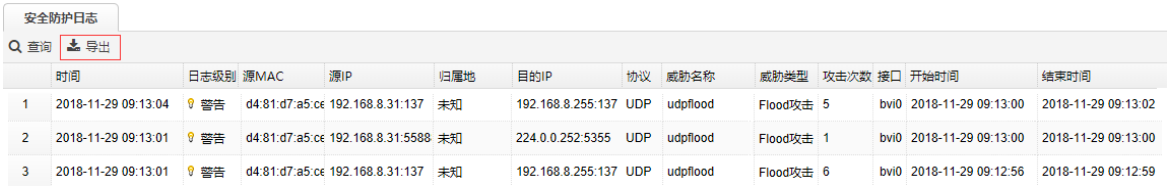
配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
日志的级别	选择一个或者多个级别的日志 • 信息 • 通知 • 警告 • 严重 • 警告
源IP地址	攻击的源IP地址
目的IP地址	攻击的目的IP地址
威胁名称	攻击的名称

配置项	说明
威胁类型	威胁的类型。总共有4种类型： • 异常包攻击 • 扫描攻击 • Flood 攻击 • ARP 攻击
协议	攻击的协议类型，比如TCP、UDP、ICMP等

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以导出所有安全防护日志到本地。

图1-46 导出安全防护日志



1.7.3 病毒防护日志

病毒防护日志记录着针对网络的 AV 攻击的日志。点击“数据中心 > 日志中心 > 安全日志 > 病毒防护日志”，进入病毒防护日志的查询界面，如图 1-47 所示。

图1-47 病毒防护日志查询页面

病毒防护日志的显示信息如表 1-37 所示：

表1-37 病毒防护日志显示信息描述表

配置项	说明
时间	日志产生的时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 紧急 • 告警 • 严重 • 错误 • 警告 • 通知 • 信息 • 调试
用户名称	用户名称
源地址	攻击的源IP地址及端口
目的地址	攻击的目的IP地址及端口
归属地	攻击的源IP所属归属地
病毒名称	病毒的名称
文件名	包含病毒的文件名称
协议类型	协议类型，分为以下几个： • HTTP • FTP • IMAP • POP3 • SMTP
行为	设备的处理行为

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-48 所示。

图1-48 病毒防护日志查询界面

病毒防护日志查询的详细信息如表 1-38 所示。

表1-38 病毒防护日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 紧急 • 告警 • 严重 • 错误 • 警告 • 通知 • 信息 • 调试
病毒名称	病毒的名称

配置项	说明
文件名	包含病毒的文件名称
用户名称	用户名称
行为	设备的处理行为
源地址	攻击的源IP地址
目的地址	攻击的目的IP地址

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以导出所有病毒防护日志到本地。

图1-49 导出病毒防护日志

1.7.4 WEB 规则防护日志

WEB 防护日志记录着针对网络的 WEB 攻击行为。点击“数据中心 > 日志中心 > 安全日志 > WEB 防护日志”，进入 WEB 防护日志的查询界面，如图 1-50 所示。

图1-50 规则防护日志查询页面

规则防护日志的显示信息如表 1-39 所示：

表1-39 规则防护日志显示信息描述表

配置项	说明
时间	日志产生的时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 紧急 • 告警 • 严重

配置项	说明
	• 错误 • 警告 • 通知 • 信息
源地址	攻击的源IP地址
归属地	攻击的源IP地址所属归属地
请求方法	攻击的请求方法
请求URL	攻击的请求URL
事件类型	WEB防护事件的类型
事件描述	事件的描述
处理动作	事件的处理动作

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-51 所示。

图1-51 规则防护日志查询界面

规则防护日志查询的详细信息如表 1-40 所示。

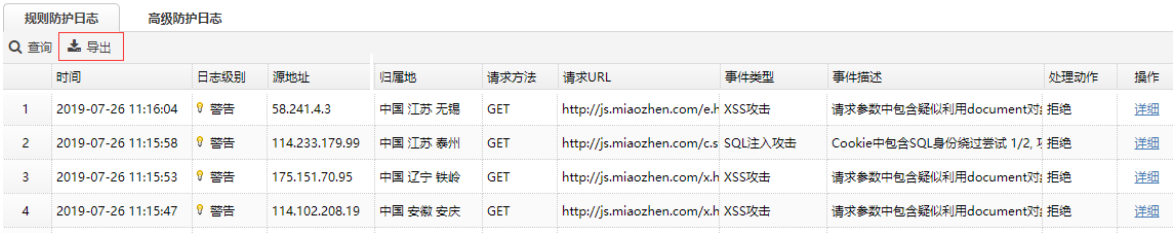
表1-40 规则防护日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
事件类型	WEB防护事件的类型
处理动作	事件处理的动作
规则ID	规则防护策略ID
事件描述	事件的描述
源地址	攻击的源 IP 地址
目的地址	攻击的目的IP地址

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以导出所有网络层攻击日志到本地。

图1-52 导出规则防护日志



1.7.5 WEB 高级防护日志

WEB 高级防护日志记录着针对网络的高级防护攻击行为。点击“数据中心 > 日志中心 > 安全日志 > WEB 防护日志>高级防护日志”，进入高级防护日志的查询界面，如图 1-53 所示。

图1-53 高级防护日志查询页面

高级防护日志的显示信息如表 1-41 所示：

表1-41 高级防护日志显示信息描述表

配置项	说明
时间	日志产生的时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 紧急 • 告警 • 严重 • 错误 • 警告 • 通知 • 信息
源地址	攻击的源IP地址
归属地	攻击的源IP地址所属归属地
请求方法	攻击的请求方法
请求URL	攻击的请求URL
事件类型	WEB防护事件的类型
事件描述	事件的描述
处理动作	事件的处理动作

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-54 所示。

图1-54 高级防护日志查询界面

高级防护日志查询的详细信息如表 1-42 所示。

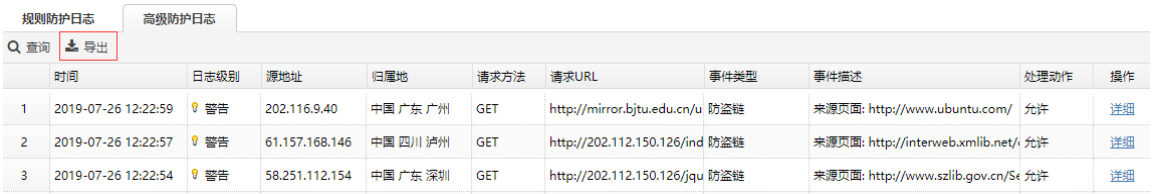
表1-42 高级防护日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
事件类型	高级防护事件的类型
处理动作	事件处理的动作
源地址	攻击的源 IP 地址
目的地址	攻击的目的IP地址

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以导出所有高级防护日志到本地。

图1-55 导出高级防护日志



1.7.6 行为模型日志

行为模型日志记录着针对网络的行为模型攻击行为。点击“数据中心 > 日志中心 > 安全日志 > 行为模型日志”，进入行为模型日志的查询界面，如图 1-56 所示。

图1-56 行为模型日志查询页面

行为模型日志的显示信息如表 1-43 所示：

表1-43 行为模型日志显示信息描述表

配置项	说明
时间	日志产生的时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 紧急 • 告警 • 严重 • 错误 • 警告 • 通知 • 信息 • 调试
源地址	攻击的源IP地址及端口
目的地址	攻击的目的IP地址及端口
归属地	攻击的目的地址所属归属地
协议类型	协议类型，比如TCP、UDP、ICMP等
行为类型	行为类型，比如 DNS 隧道等
详细信息	行为模型攻击的详细信息
行为描述	行为模型攻击的描述
动作	设备处理动作

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-57 所示。

图1-57 行为模型日志查询界面

行为模型日志查询的详细信息如表 1-44 所示。

表1-44 行为模型日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 紧急 • 告警 • 严重 • 错误 • 警告 • 通知 • 信息 • 调试
行为	设备处理的行为
源IP地址	攻击的源IP地址
目的IP地址	攻击的目的IP地址

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以导出所有行为模型日志到本地。

图1-58 导出行为模型日志

1.7.7 防暴力破解日志

防暴力破解日志记录着针对网络的防暴力破解攻击行为。点击“数据中心 > 日志中心 > 安全日志 > 防暴力破解日志”，进入防暴力破解日志的查询界面，如图 1-59 所示。

图1-59 防暴力破解日志查询页面

防暴力破解日志的显示信息如表 1-45 所示：

表1-45 防暴力破解日志显示信息描述表

配置项	说明
时间	日志产生的时间
源地址	攻击的源IP地址
归属地	攻击的源IP地址所属的归属地
目的地址	攻击的目的IP地址
服务	防暴力破解服务类型
破解成功	破解是否成功
破解账号	破解的账号名称
防御动作	设备处理的行为

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-60 所示。

图1-60 防暴力破解日志查询界面

防暴力破解日志查询的详细信息如表 1-46 所示。

表1-46 防暴力破解日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
源IP地址	攻击的源IP地址
目的IP地址	攻击的目的IP地址
服务	防暴力破解服务类型
破解成功	破解是否成功
破解账号	破解的账号名称
防御动作	设备处理的行为

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以导出所有防暴力破解日志到本地。

图1-61 导出防暴力破解日志

	时间	源地址	归属地	目的地址	服务	破解成功	破解账号	防御动作
1	2020-09-23 15:35:57	192.168.1.2	局域网	123.129.242.140	http	否		加入黑名单
2	2020-09-21 17:45:27	192.168.1.2	局域网	123.129.242.140	http	否		加入黑名单
3	2020-09-21 07:35:05	192.168.1.2	局域网	123.129.242.140	http	否		加入黑名单

1.7.8 弱密码防护日志

弱密码防护日志记录着针对网络的弱密码防护行为。点击“数据中心 > 日志中心 > 安全日志 > 弱密码防护日志”，进入弱密码防护日志的查询界面，如图 1-62 所示。

图1-62 弱密码防护日志查询页面

	时间	源地址	服务器地址	服务	用户名称	弱密码类型
	时间	源地址	服务器地址	服务	用户名称	弱密码类型
1	2019-07-26 03:31:12	192.168.203.40	192.168.0.253	ftp	anonymous	密码与用户名相同
2	2019-07-26 00:52:00	172.21.0.220	192.168.2.75	ftp	xdftpnd	密码长度小于等于8 且为字典序
3	2019-07-26 00:48:24	172.21.0.220	192.168.2.75	ftp	xdftpnd	密码长度小于等于8 且为字典序
4	2019-07-26 00:38:52	172.21.0.220	192.168.2.75	ftp	xdftpnd	密码长度小于等于8 且为字典序
5	2019-07-26 00:38:18	172.21.0.220	192.168.2.75	ftp	xdftpnd	密码长度小于等于8 且为字典序
6	2019-07-26 00:36:13	172.21.0.220	192.168.2.75	ftp	xdftpnd	密码长度小于等于8 且为字典序

弱密码防护日志的显示信息如表 1-47 所示：

表1-47 弱密码防护日志显示信息描述表

配置项	说明
时间	日志产生的时间
源地址	攻击的源IP地址
服务器地址	服务器IP地址
服务	防护的服务类型
用户	登录的用户名
弱密码类型	弱密码的类型

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-63 所示。

图1-63 弱密码防护日志查询界面

弱密码防护日志查询的详细信息如表 1-48 所示。

表1-48 弱密码防护日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
源地址	攻击的源IP地址
服务器地址	服务器的IP地址
服务	防护的服务类型
用户	登录的用户名

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以导出所有弱密码防护日志到本地。

图1-64 导出弱密码防护日志

1.7.9 非法外联防护日志

非法外联防护日志记录着针对网络的非法外联防护攻击行为。点击“数据中心 > 日志中心 > 安全日志 >非法外联防护日志”，进入非法外联防护日志的查询界面，如图 1-65 所示。

图1-65 非法外联防护日志查询页面

非法外联防护日志的显示信息表 1-49 如所示：

表1-49 非法外联防护日志显示信息描述表

配置项	说明
时间	日志产生的时间
名称	非法外联防护策略名称
服务器地址	服务器IP地址
外联地址	服务器主动外联地址
归属地	服务器主动外联地址所属归属地
端口	服务器主动外联的端口
协议	服务器主动外联地址的协议，比如TCP、UDP、ICMP等
行为	设备处理动作

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-66 所示。

图1-66 非法外联防护日志查询界面

非法外联防护日志查询的详细信息表 1-50 如所示。

表1-50 非法外联防护日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
名称	非法外联防护策略名称
服务器地址	服务器IP地址
外联地址	服务器主动外联地址
行为	设备处理的动作
协议	服务器主动外联地址的协议，比如TCP、UDP、ICMP等
端口	服务器主动外联的端口

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可以导出所有非法外联防护日志到本地。

图1-67 导出非法外联防护日志

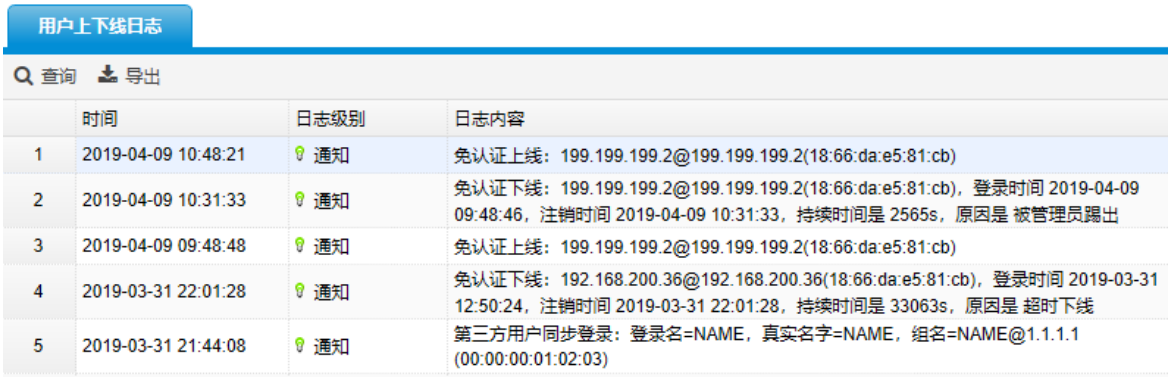
	时间	名称	服务器地址	外联地址	归属地	端口	协议	行为
1	2019-07-26 13:28:33	非法外联	192.168.0.200	10.222.1.47	局域网	445	TCP	允许
2	2019-07-26 13:28:30	非法外联	192.168.0.200	10.222.1.26	局域网	445	TCP	允许

1.8 终端日志

1.8.1 用户上下线日志

用户上下线日志记录认证用户上下线的日志信息，点击“数据中心 > 日志中心 > 终端日志 > 用户上下线日志”，进入用户上下线日志日志的查询界面，如图 1-68 所示。

图1-68 用户上下线日志查询页面



	时间	日志级别	日志内容
1	2019-04-09 10:48:21	通知	免认证上线：199.199.199.2@199.199.199.2(18:66:da:e5:81:cb)
2	2019-04-09 10:31:33	通知	免认证下线：199.199.199.2@199.199.199.2(18:66:da:e5:81:cb)，登录时间 2019-04-09 09:48:46，注销时间 2019-04-09 10:31:33，持续时间是 2565s，原因是 被管理员踢出
3	2019-04-09 09:48:48	通知	免认证上线：199.199.199.2@199.199.199.2(18:66:da:e5:81:cb)
4	2019-03-31 22:01:28	通知	免认证下线：192.168.200.36@192.168.200.36(18:66:da:e5:81:cb)，登录时间 2019-03-31 12:50:24，注销时间 2019-03-31 22:01:28，持续时间是 33063s，原因是 超时下线
5	2019-03-31 21:44:08	通知	第三方用户同步登录：登录名=NAME，真实名字=NAME，组名=NAME@1.1.1.1 (00:00:00:01:02:03)

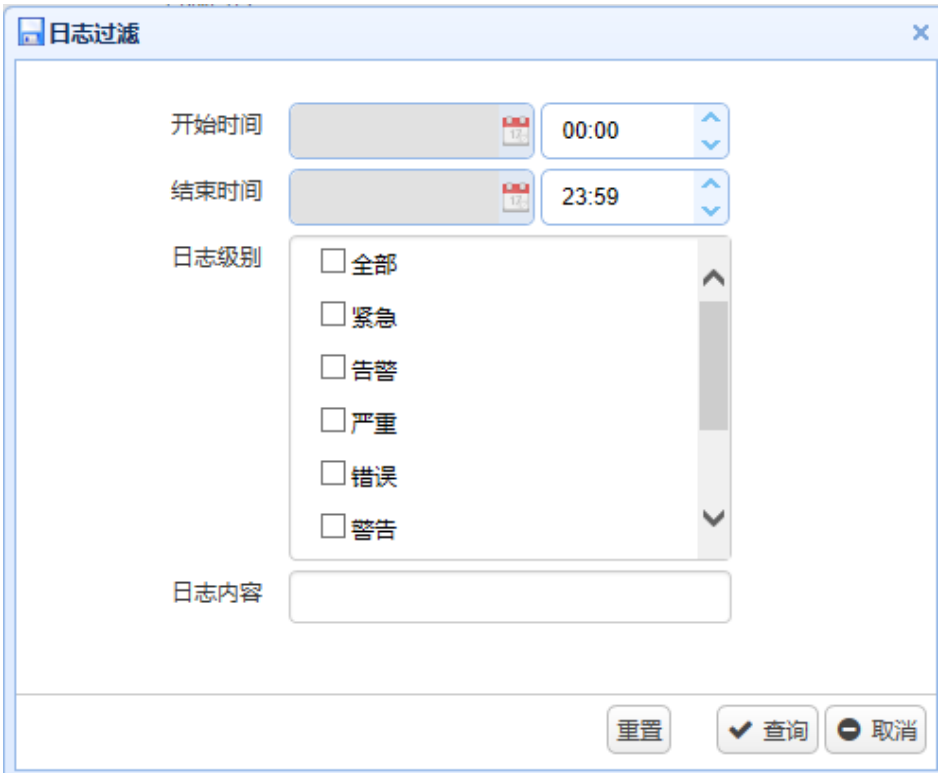
用户上下线日志的显示信息如表 1-51 所示：

表1-51 用户上下线日志显示信息描述表

配置项	说明
时间	日志产生的时间
日志级别	根据严重程度的不同，日志分为以下几个级别： • 信息 • 通知 • 警告 • 严重 • 警告
日志内容	用户上下线日志的内容

点击<查询>按钮，可以查看根据设定的条件，查询关心的日志，如图 1-69 所示。

图1-69 用户上下线日志查询界面



用户上下线日志查询的详细信息如表 1-52 所示。

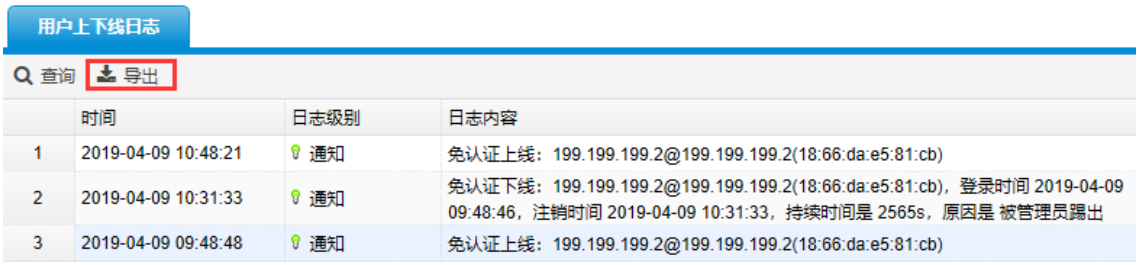
表1-52 用户上下线日志查询详细信息

配置项	说明
开始时间	日志的最早发生时间
结束时间	日志的最晚发生时间
日志级别	选择一个或者多个级别的日志 • 信息 • 通知 • 警告 • 严重 • 警告
日志内容	用户上下线日志的内容，支持模糊查询

点击<查询>按钮之后，可以显示出符合设置条件的日志。

点击<导出>按钮后，可导出所有系统日志。

图1-70 导出用户上下线日志



1.8.2 共享接入日志

通过菜单“数据中心 > 日志中心 > 终端日志 > 共享接入日志”，进入如图 1-71 所示页面。在该页面上可以查看设备监控共享上网被惩罚阻断或限速的日志。

图1-71 共享接入日志

共享接入日志各项参数含义如表 1-53 所示。

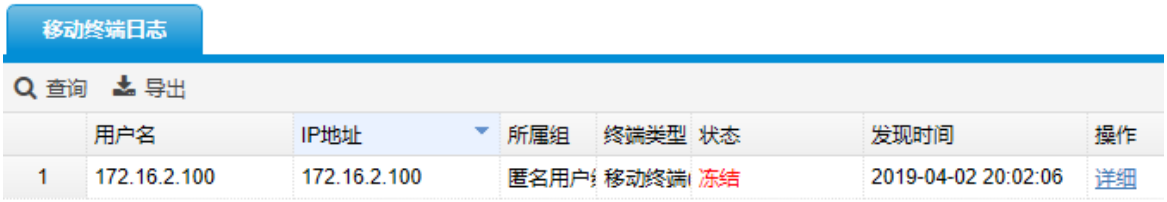
表1-53 共享接入日志含义表

标题项	说明
用户名	显示设备存储ip地址对应的用户名。
所属组	显示设备存储用户加入的用户组。
IP	显示终端IP地址。
用户mac	显示终端MAC地址。
终端数量	共享设备下面的终端数量。
惩罚方式	惩罚方式只有阻断或限速两种。
发现时间	显示发现共享接入用户的时间。
操作	选择详细可查看共享终端用户的识别明细。

1.8.3 移动终端日志

通过菜单“数据中心 > 日志中心 > 终端日志 > 移动终端日志”，进入如图 1-72 所示页面。在该页面上可以查看移动终端接入的日志信息。

图1-72 移动终端日志



移动终端日志各项参数含义如表 1-54 所示。

表1-54 移动终端日志含义表

标题项	说明
用户名	设备记录的移动终端用户名。
IP地址	设备记录的移动终端IP地址。
所属组	移动终端用户所属用户组。
终端类型	设备记录的移动终端型号。
状态	移动终端状态： • 正常：只检测，不进行冻结； • 冻结：移动终端被冻结。
发现时间	移动终端检测发现的时间。
操作	选择详细可查看移动终端日志的明细。

1.8.4 流量限额日志

通过菜单“数据中心 > 日志中心 > 终端日志 > 流量限额日志”，进入流量限额日志页面。在该页面上可以查看用户流量限额策略产生的日志信息。

图1-73 流量限额日志

移动终端日志各项参数含义如表 1-54 所示。

表1-55 移动终端日志含义表

标题项	说明
用户名	产生日志的终端用户名。
所属组	用户所属的用户组名称。

用户mac	产生日志的用户MAC地址。。
策略名称	匹配到的用户限额策略名称。
行为类别	行为类别，如违规行为等。
事件类型	流量限额事件的类型，如流量违规等。
动作	设备的处理动作
级别	日志的级别
时间	日志产生的时间。
操作	选择详细可查看日志的明细。

1.9 日志导出

1.9.1 概述

日志支持导出功能，审计日志、应用控制日志、恶意 URL 日志等可以根据时间范围选择要导出的日志；系统日志、操作日志可以直接导出全部查询结果。

1.9.2 系统日志导出

在导航栏中选择“数据中心>日志中心>系统日志”，进入系统日志页面，如图 1-74 所示。

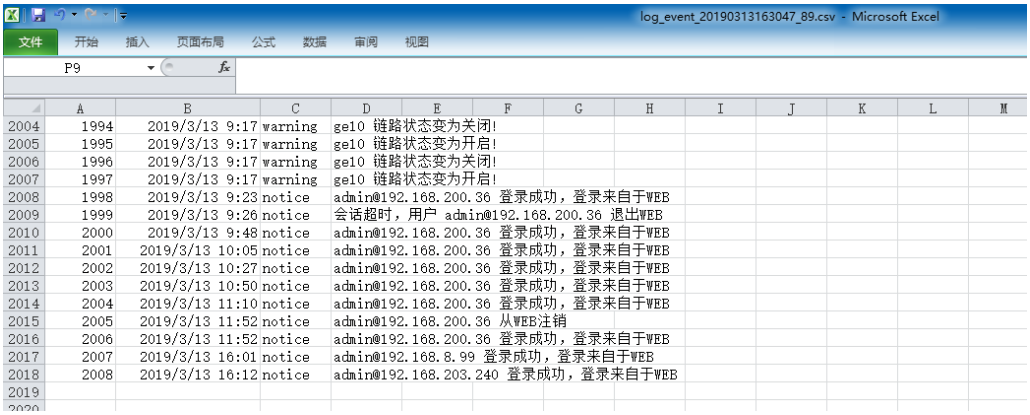
图1-74 系统日志页面

表1-56 系统日志界面详细说明

项目	说明
查询	查询日志
导出	导出日志

单击<导出>，可以导出 CSV 格式的日志，如图 1-75 所示。

图1-75 系统日志导出



1.9.3 审计日志导出

在导航栏中选择“数据中心>日志中心>审计日志>IM 聊天软件日志”，进入 IM 聊天软件日志页面，如图 1-76 所示。

图1-76 IM 聊天软件日志页面

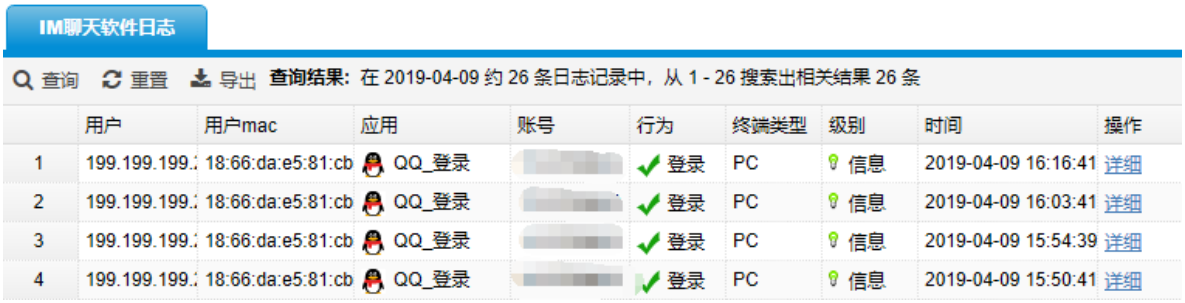


表1-57 IM 聊天软件日志界面详细说明

项目	说明
查询	查询日志
重置	重置到初始页面
导出	导出日志

单击<导出>，在弹出的过滤框中选择需要导出的日志的时间范围，单击<导出>，即可将对应时间段的日志压缩包下载到本地。解压缩后，可以看到带有日期信息的 CSV 文件。如图 1-77、图 1-78 所示。

图1-77 导出过滤

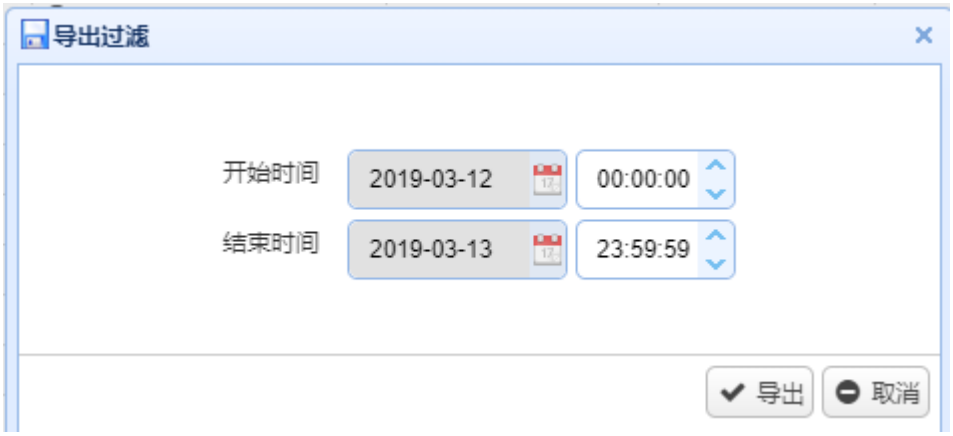
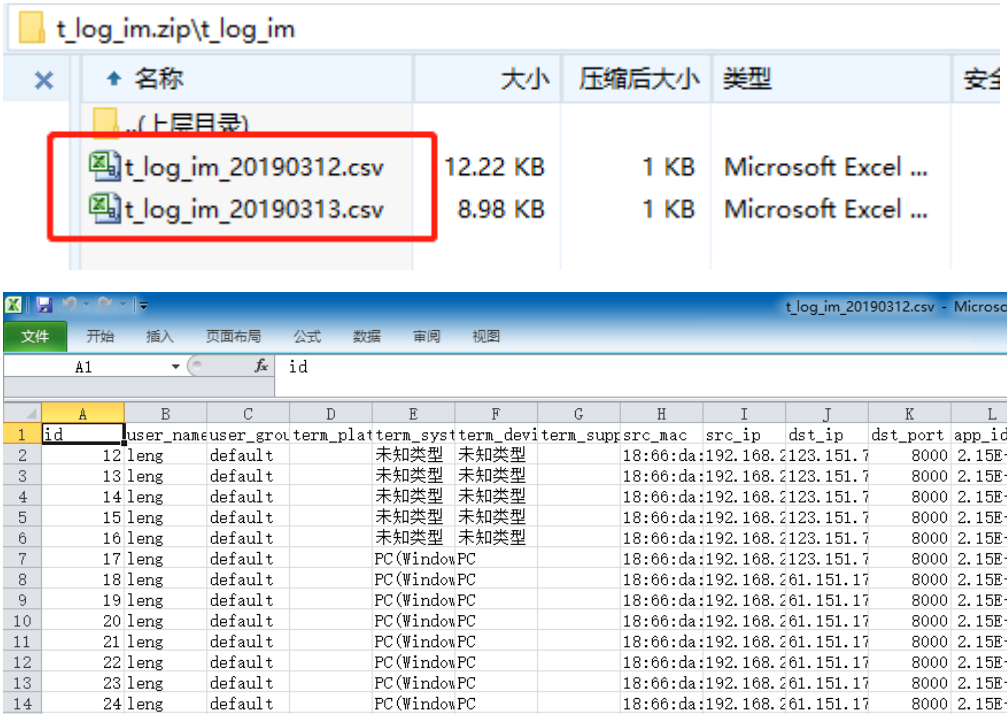


图1-78 审计日志导出的文件



id	user_name	user_grou	term_plat	term_syst	term_devi	term_supp	src_mac	src_ip	dst_ip	dst_port	app_id	app_name	app_
12	leng	default		未知类型	未知类型		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
13	leng	default		未知类型	未知类型		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
14	leng	default		未知类型	未知类型		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
15	leng	default		未知类型	未知类型		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
16	leng	default		未知类型	未知类型		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
17	leng	default		PC(Window	PC		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
18	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
19	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
20	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
21	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
22	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
23	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
24	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I

1.10 日志典型配置举例

1.10.1 日志典型配置举例

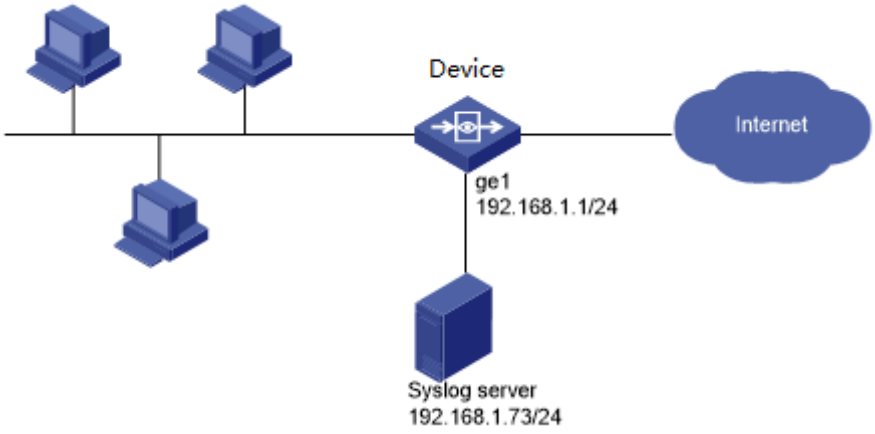
1. 组网需求

- 配置一台日志服务器接收日志，IP 地址是 192.168.1.73，端口是 9988。

- 配置本地不记录操作日志，并且将告警级别以上的操作日志发送到日志服务器。

2. 组网图

图1-79 配置日志组网图



3. 配置步骤

(1) 配置日志服务器，点击“系统管理 > 系统设定 > 日志设定 > 日志服务器”，进入日志服务器的配置页面，日志服务器的 IP 为 192.168.1.73，端口为 9988，并勾选启用，如图 1-80 所示。点击<提交>按钮，完成日志服务器的配置。

图1-80 配置日志服务器

点击“系统管理 > 系统设定 > 日志设定 > 日志过滤”，进入日志过滤的配置页面，将操作日志后面的本地日志改为不记录，Server 日志改为发送，告警，如图 1-81 所示。点击<提交>按钮，完成日志过滤的配置

图1-81 日志过滤配置界面

4. 验证配置

执行告警级别以上的操作，不能从本地查询到操作日志，可以从日志服务器上查询到操作日志。

目 录

1 HA ····· 1-1
1.1 概述 ····· 1-1
1.1.1 HA 简介 ····· 1-1
1.1.2 HA 组网模式 ····· 1-1
1.1.3 HA 工作状态 ····· 1-2
1.1.4 接口概念 ····· 1-2
1.1.5 抢占模式 ····· 1-3
1.1.6 抢占延时定时器 ····· 1-3
1.1.7 心跳报文 ····· 1-3
1.1.8 HA 管理地址 ····· 1-3
1.1.9 HA 状态同步 ····· 1-3
1.1.10 HA 状态切换 ····· 1-4
1.2 配置 HA ····· 1-4
1.2.1 配置概述 ····· 1-4
1.2.2 HA 全局配置 ····· 1-5
1.2.3 HA 状态显示和维护 ····· 1-6
1.2.4 配置管理地址 ····· 1-8
1.3 HA 配置举例 ····· 1-9
1.3.1 HA 主备模式配置举例 ····· 1-9
1.3.2 HA 主主模式配置举例 ····· 1-14

1 HA

1.1 概述

1.1.1 HA 简介

HA 是 High Availability 的缩写，即高可用性，可防止网络中由于单个网关产品的设备故障或链路故障导致网络中断，保证网络服务的连续性和安全强度。

随着网络的快速普及和应用的日益深入，各种增值业务（如 IPTV、视频会议等）得到了广泛部署，网络中断可能影响大量业务、造成重大损失。因此，作为业务承载主体的基础网络，其可靠性日益成为受关注的焦点。

在实际网络中，总避免不了各种非技术因素造成的网络故障和服务中断。因此，提高系统容错能力、提高故障恢复速度、降低故障对业务的影响，是提高系统可靠性的有效途径。

本产品通过双机热备来实现 HA。

说明

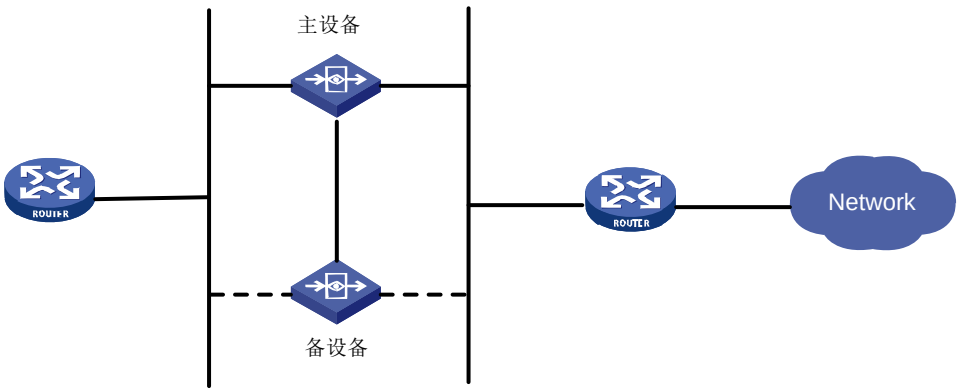
进行 HA 的两台设备，要求为同一个硬件型号，并且选择同样的接口作为 HA 接口。这两台设备之间通过 HA 接口直连，HA 接口可以是任何以太网接口，也可以是 AGG 接口（聚合接口）。

1.1.2 HA 组网模式

目前产品支持两台网关设备以主-备或主主模式运行。

主备模式是指实现 HA 的两台设备中，一台作为主设备，另外一台作为备设备。主设备在进行业务的同时，将相关的配置和数据信息实时同步到备设备。当主设备出现故障或主设备的链路中断时，备用设备成为主设备，接管原主设备的工作，实现网络业务的无缝切换。如图 1-1 所示。

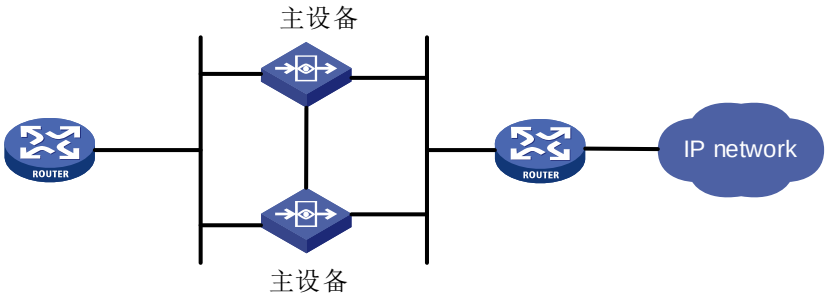
图1-1 主备模式



在主备模式下，主设备响应各类报文请求，并且转发网络流量；备用设备不响应报文请求，也不转发网络流量。主备设备之间通过 HA 心跳线同步状态信息，配置信息以及特征库文件。

在主主模式下，两台设备都配置成主动，使两台设备同时运行各自的工作，且相互监测对方的情况。当其中一台设备发生故障时，另外一台设备运行其自身的工作并且接管故障设备的工作，以保证整体业务不间断。兼具故障备份和负载均衡。如图 1-2 所示。

图1-2 主主模式



主备模式和主主模式均支持路由模式和透明模式。

- 路由模式：设备接口配置 IP 地址，通过路由转发数据，上下游设备的接口 IP 地址处于不用网段。
- 透明模式：设备接口配置加入桥中，只有桥接口配置 IP 地址，通过桥转发数据，上下游设备的接口 IP 地址处于同一网段，不知道设备的存在。

说明

HA 的主主模式的路由部署方式中——HA 设备的上下行可以在不同的网段。但是由于一台出现故障，另一台需要代理故障设备的流量发送免费 ARP 更新上下游的 ARP 表项。所以需要 HA 设备的上下联接口网段和与之相连的其它设备网络相同。

1.1.3 HA 工作状态

HA 主备模式的工作状态主要有两种，主模式和备模式。

- 主模式是指在设备 HA 主备模式中，实际参与工作。
- 备模式是指设备是指在 HA 主备模式中，作为主设备备份，不参与实际工作。只有当主设备失效，才转换为主设备，接替其工作。

HA 主主的工作状态有三种：Master 模式、Master（N）模式、Master（A）模式。

- Master 模式：两台设备都处于流量转发状态。
- Master（N）模式：本端设备出现故障。
- Master（A）模式：本端设备代理故障设备和自己原来的所有流量。

1.1.4 接口概念

HA 中，主要有两种接口概念。

- HA 接口：连接两台 HA 设备的接口，不参与报文的转发，只用于 HA 设备直接心跳报文和同步报文发送。

- 监控接口：HA 必须重点关注的设备接口，如果此接口状态为 down，表明网络状态发生故障，需要切换主备设备来修复故障。

1.1.5 抢占模式

- 非抢占方式：如果备份组中的设备工作在非抢占方式下，则只要主设备没有出现故障，备设备不会主动成为主设备。
- 抢占模式：抢占模式时指用户可以根据需要，指定某一台设备优选为主设备或者为备设备。如果配置优选为主设备的设备工作正常，即使当前设备为备状态，也要“抢占”成主设备。

说明

- HA 的两台设备在主备模式下：抢占模式必须匹配，或者全部配置成非抢占模式，或者一个配置成抢占为主，一个配置成抢占为备，否则 HA 无法正确协商。
- HA 的主主模式两台设备没有抢占的概念。

1.1.6 抢占延时定时器

在 HA 主备模式下：为了避免 HA 设备频繁进行主备状态转换，备设备在网络状态恢复为正常状态后，也不会马上抢占为主，而是在流表等信息同步完成后，等待一定时间。只有在这段时间内，设备依然正常，才会通知备设备，抢占成主。

在 HA 主主模式下，没有抢占的概念。

1.1.7 心跳报文

HA 设备之间用来相互通告设备的 HA 配置和 HA 状态的报文。如果一个设备在规定时间没有收到邻居心跳报文，可以认定 HA 邻居已经失效。

1.1.8 HA 管理地址

处于备状态的 HA 设备不会参与网络转发，因此无法通过其接口配置的 IP 地址访问。为了解决这一问题，可以在设备上配置管理地址，用作备设备的网络管理。用户可以从外部访问备设备的 telnet 服务和 web 管理界面。

说明

在 HA 主备和主主模式下，建议两台设备都配置管理地址。目的是防止当其中一台设备故障不转发数据的情况下，依然可以通过管理地址进行管理。

1.1.9 HA 状态同步

HA 作为热备份，为了在状态切换的过程中，尽量减小对网络的影响。HA 会将主设备上的一些实时的状态同步给备设备。同步的内容主要包括三种：session 信息、设备配置、特征库。

- Session 信息：包括设备连接表、FBD、用户信息、PKI。
- 设备配置：同步的设备配置中不包含 HA 配置信息，以及一些特殊的配置。
- 特征库：特征库包括 APP 特征库以及 URL 特征库。

HA 主主模式下，同步内容有 2 种：运行状态同步、监控接口地址同步。

- Session 信息：包括设备连接表、FBD、用户信息、PKI。
- 监控接口地址同步：当其中一台 HA 主主设备发生故障，那么另一台会代理这台故障设备的 IP 地址。

1.1.10 HA 状态切换

- 当设备启用 HA 主备模式后，设备进入 init（初始化状态）。在这个状态，设备不参与报文转发，只接受对端 HA 设备的 keepalive 报文。如果收到了主设备发出的 keepalive 报文，设备会进入备状态。如果没有收到 keepalive 报文，设备会进入主状态。
- 如果设备成为主状态后，会向外发送免费 arp 报文，用来更新上下游设备的 arp 表（工作在路由模式），或者向外发送特殊的报文刷新上下游交换机的 FBD 信息（工作在桥模式）。
- 如果设备成为备设备，设备会清除自己的 FBD 表（如果工作在桥模式），并且向主设备请求状态信息。
- HA 主主的两台设备，默认都是 Master 的状态，两台设备同时在转发流量。
- HA 主主的两台设备，其中一台发生故障，故障设备的状态机会变成 Master（N），不再转发数据；另外一台设备的状态机变成 Master（A），开始代理这台设备的全部流量。

注意

- 如果设备工作在桥模式，为了防止形成环路，在刚刚成为主设备的一秒内，桥不转发报文。
- 如果设备工作在桥模式，在成为备设备后，设备会将加入桥的接口关闭打开一次，用来刷新上下游交换机的 FBD 表。
- 设备刚变成备状态，会从主设备获取配置信息，但是不会立刻加载。如果主备设备的信息不一致。需要重启备设备。

1.2 配置HA

1.2.1 配置概述

HA 配置的推荐步骤如表 1-1 所示。

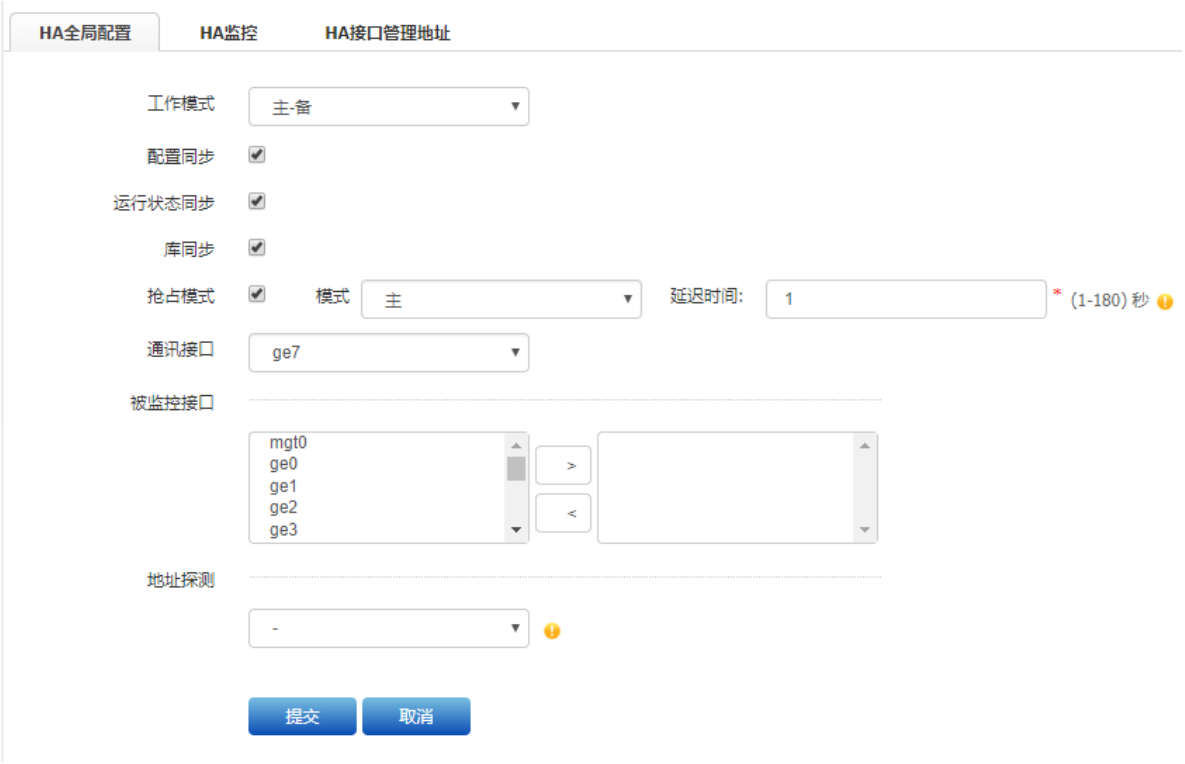
表1-1 HA 配置的推荐步骤

配置任务	说明	详细配置
HA全局配置	必选	• 1.2.2
HA状态查看和维护	可选	• 1.2.3
配置管理地址	可选	• 1.2.4

1.2.2 HA 全局配置

在导航栏中选择“系统管理 > 系统设定 > 高可用性 > HA 全局配置”，进入 HA 的配置页面，如图 1-3 所示。

图1-3 HA 全局配置页面



页面的详细说明如表 1-2。

表1-2 HA 全局配置的详细说明

项目	说明
工作模式	HA的工作模式，有不启用、主备模式、主主模式三个选项。
配置同步	是否启用HA配置同步。
运行状态同步	是否配置HA运行状态同步。
库同步	是否配置HA库同步。
抢占模式	是否配置HA抢占模式。
模式	HA的抢占模式，有主和备两个选项。
延时时间	HA抢占延时时间。
HA通讯接口	HA 的通讯接口，只能选择物理接口和聚合接口。
被监控接口	HA监控的接口。
地址探测	选择引用地址探测对象。地址探测出接口需配置管理IP且到探测IP可达，非共享网络地址探测不建议配置地址

项目	说明
	探测。

选中左边的接口列表中的接口，点击<添加>按钮，可以将选中接口配置成到监控接口。

选中右边的监控接口列表中的接口，点击<删除>按钮，可以将选中接口从监控接口列表中删除。

输入完毕后，点击<提交>按钮，应用配置。

说明

- HA 主备模式下，如果开启地址探测，地址探测出接口需配置管理 IP 且到探测 IP 可达。主机使用接口主地址发包进行探测，备机是使用 HA 接口管理地址发包进行探测，因此，备机上需要配置 HA 接口管理地址，否则备机无法探测成功，主备无法进行切换。当主备切换后，原来的主机切换为新的备机，同理，原来的主机也需要配置 HA 接口管理地址，否则新的备机无法进行地址探测。
- HA 主主模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用主地址发包，但是发生状态切换变成 master(N)状态后，地址探测就会用管理地址发包了。
- 开启地址探测功能后，在配置源 NAT 时，要将管理 IP 的地址排除，避免管理地址过出接口时做源 NAT 导致探测报文发不出去，因为在 HA 备状态下，备机是使用 HA 接口管理地址发包进行探测，探测报文源地址为管理 IP 时才会发送，否则探测报文无法发送，如果不将管理 IP 的地址排除，源 NAT 会改变探测报文源地址，导致探测报文发不出去。

1.2.3 HA 状态显示和维护

在导航栏中选择“系统管理 > 系统设定 > 高可用性 > HA 全局配置”，点击页面上方的“HA 监控”标签，进入 HA 监控页面，如图 1-4 所示。

图1-4 HA 监控页面

页面的详细说明如表 1-3。

表1-3 HA 监控的详细说明

项目	说明
设备名称	本地设备和HA邻居设备的设备名称。
主备状态	本地设备和HA邻居设备的HA状态。
系统配置	本地设备和HA邻居设备的配置是否同步。
IPS库	本地设备和HA邻居设备的IPS特征库是否同步。
AV库	本地设备和HA邻居设备的AV特征库是否同步。
APP库	本地设备和HA邻居设备的APP特征库是否同步。

点击<同步配置>按钮，可以将主设备的配置同步给备设备，并且重启备设备。

点击<主备切换>按钮，可以手动切换主备设备的 HA 状态。

说明

- 如果系统配置已经相同，无需再次同步，<同步配置>按钮无法点击。
- 如果配置了抢占模式，无法进行手动切换状态，<主备切换>按钮无法点击。

1.2.4 配置管理地址

在导航栏中选择“系统管理 > 系统设定 > 高可用性 > HA 全局配置”，点击页面上方的“HA 接口管理地址”标签，进入 HA 接口管理地址配置页面，如图 1-5 所示。

图1-5 HA 接口管理地址页面

页面的详细说明如表 1-4。

表1-4 HA 接口管理地址的详细说明

项目	说明
接口名称	配置管理地址接口名称。
管理地址	接口配置的管理地址。
操作	对管理地址可进行的操作。

点击<新建>按钮，进入 HA 接口管理地址的新建页面，如图 1-6 所示。

图1-6 HA 接口管理地址新建页面

页面的详细说明如表 1-5。

表1-5 HA 接口管理地址的详细说明

项目	说明
接口名称	配置管理地址接口名称，只包含物理接口，桥接口和三层子接口。
管理地址	接口配置的管理地址，仅支持IPv4地址。

输入完毕后，点击<提交>按钮，应用配置。

在 HA 接口管理地址显示页面，可以点击管理地址右边的<删除>按钮，删除对应的管理地址。

1.3 HA配置举例

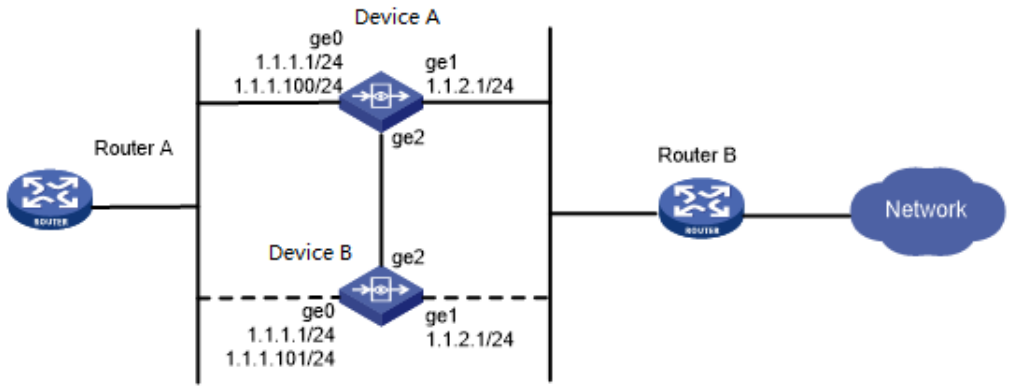
1.3.1 HA 主备模式配置举例

1. 组网需求

- 设备 A 配置为主设备，设备 B 配置成为备设备。
- 设备 A 的 ge2 接口作为 HA 接口和设备 B 的 ge2 接口相连。
- 设备 A 配置为抢占主模式，设备 B 配置成抢占备模式。
- 设备 A 和设备 B 的 keepalive 间隔设置为 1 秒，重试次数为 3 次。
- 设备 A 和设备 B 配置 ge0 和 ge1 为监控接口。
- 设备 A 和设备 B 配置自动同步 session，配置特征库。

2. 组网图

图1-7 HA 主备模式组网图



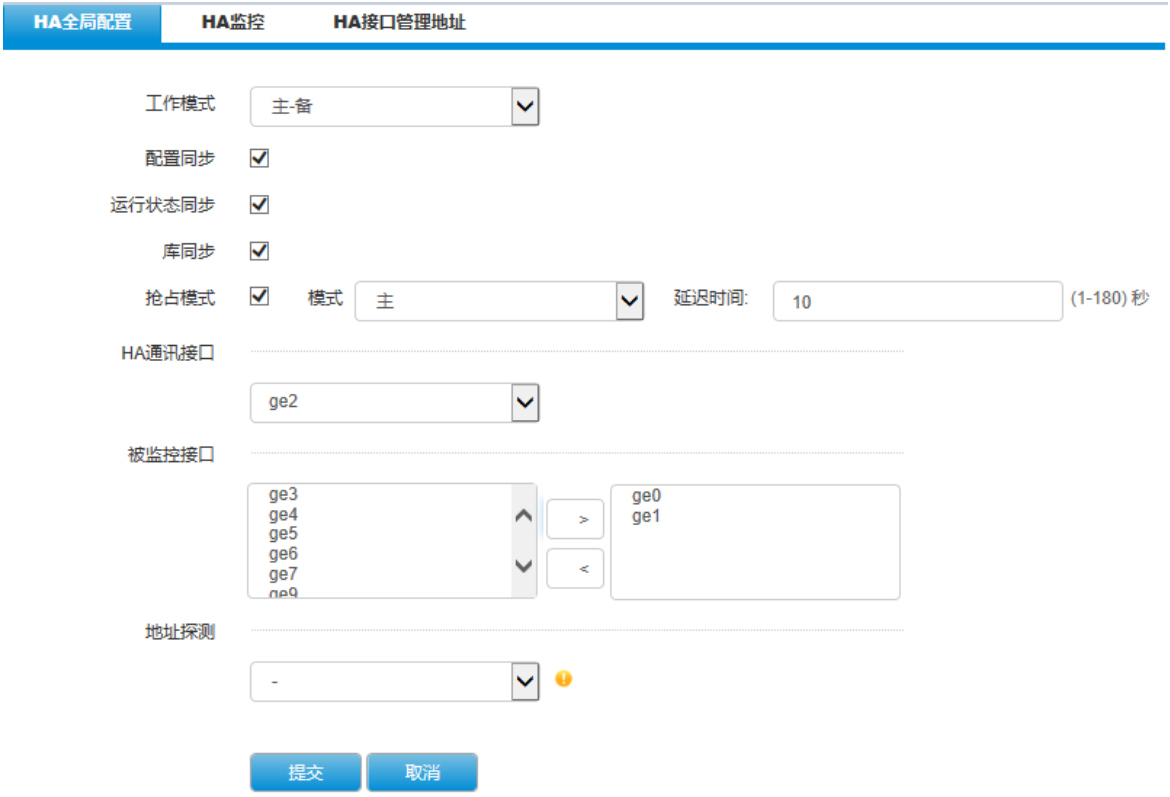
3. 配置思路

- 配置设备 A 为主设备，设备 B 为备设备。
- 设备 A 监控自己的 ge0 和 ge1 接口，当 ge0 或者 ge1 down 后，设备 A 切换成备状态，设备 B 切换成主状态。
- 设备 B 监控设备 A 的状态，当 B 收不到 A 的心跳报文，认为设备 A 已经失效，设备 B 变成主状态。
- 当设备 A 的状态恢复正常后，设备 A 会抢回自己的主状态。设备 A 变成主设备，设备 B 变成备设备。

4. 配置步骤

(1) 配置设备 A 的 HA 全局配置。

图1-8 设备 A 的 HA 全局配置

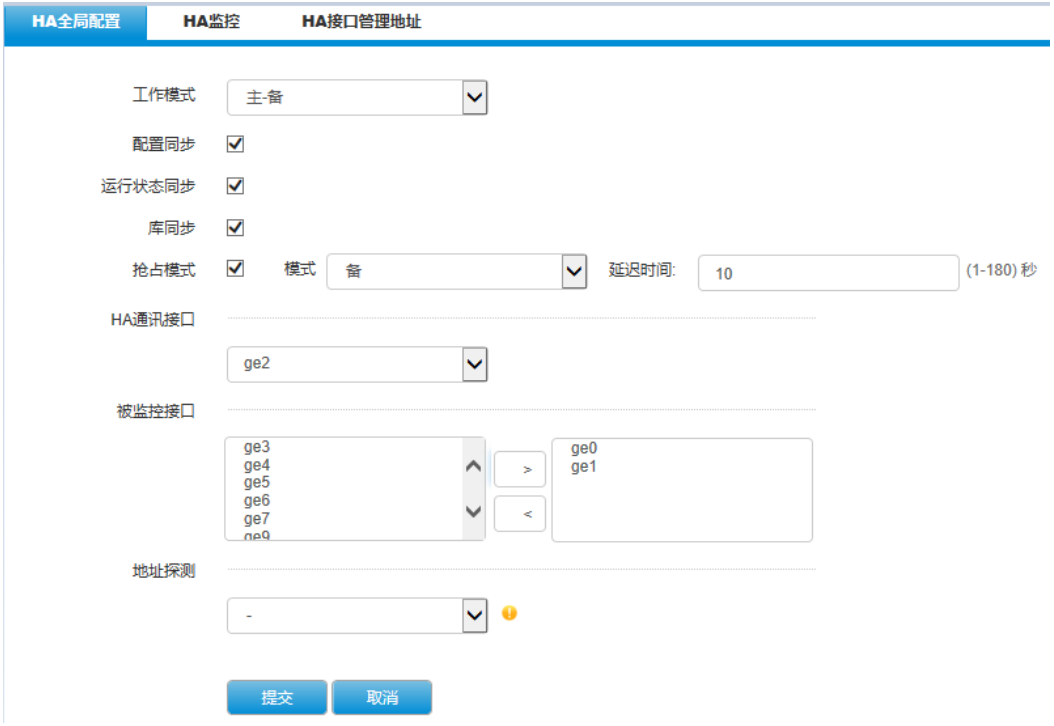


(2) 在设备 A 的 ge0 接口配置管理地址 1.1.1.100/24。

图1-9 配置设备 A 的管理地址

(3) 配置设备 B 的 HA 全局配置。

图1-10 设备 B 的 HA 全局配置



(4) 在设备 B 的 ge0 接口配置管理地址 1.1.1.101/24。

图1-11 配置设备 B 的管理地址

(5) 点击设备 A 的 HA 监控页面的配置同步按钮，同步配置。

图1-12 设备 A 的 HA 监控页面

5. 验证配置

(1) 通过管理地址 1.1.1.100/24 访问设备 A，查看 HA 监控页面。

图1-13 设备 A 的 HA 监控页面显示

(2) 通过管理地址 1.1.1.101/24 访问设备 B，查看 HA 监控页面。

图1-14 设备 B 的 HA 监控页面显示

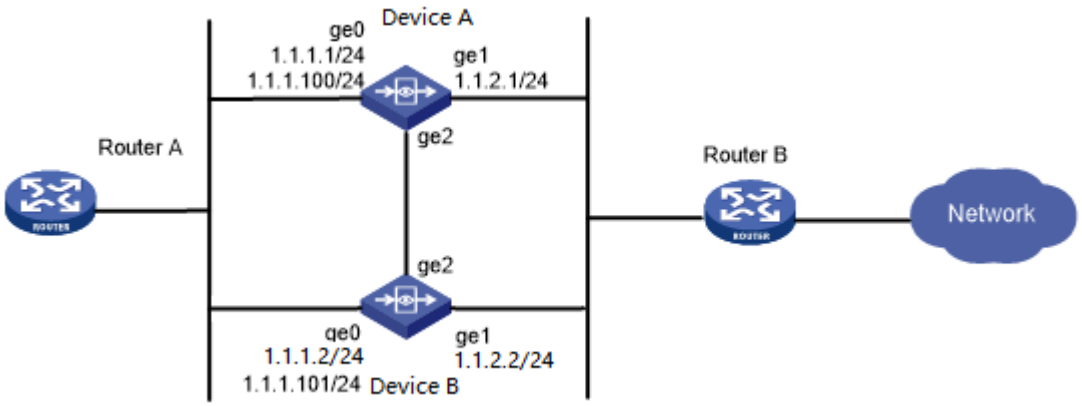
1.3.2 HA 主主模式配置举例

1. 组网需求

- 设备 A 配置为主设备，设备 B 配置成为主设备。
- 设备 A 的 ge2 接口作为 HA 接口和设备 B 的 ge2 接口相连。
- 设备 A 和设备 B 配置 ge0 和 ge1 监控接口。
- 设备 A 和设备 B 配置自动同步 session，自动同步监控接口地址。

2. 组网图

图1-15 HA 主主模式组网图



3. 配置思路

- 配置设备 A 为主设备，设备 B 也为主设备。
- 设备 A 监控自己的 ge0 和 ge1 接口，当 ge0 或者 ge1 down 后，设备 A 切换成主故障状态（Master N），不再转发数据。设备 B 切换成全主状态（Master A ）,继续处理设备 A 之前承载的业务，保证业务不中断。
- 设备 B 监控设备 A 的状态，当 B 收不到 A 的心跳报文，认为设备 A 已经失效，设备 B 变成全主状态（Master A ）。
- 当设备 A 的状态恢复正常后，设备 A 会抢回自己的主状态，由原来的故障状态 Master N 状态切回 Master 状态。设备 A 变成主设备，设备 B 由原来承载所有流量的 Master A 状态切回正常的 Master 状态。
- 主主模式下，设备上没有一键同步配置功能，需要管理员自己保证主主模式下两台设备的配置一样。

4. 配置步骤

(1) 配置设备 A 的 HA 全局配置。

图1-16 设备 A 的 HA 全局配置

(2) 在设备 A 的 ge0 接口配置管理地址 1.1.1.100/24。

图1-17 配置设备 A 的管理地址

(3) 配置设备 B 的 HA 全局配置。

图1-18 设备 B 的 HA 全局配置

(4) 在设备 B 的 ge0 接口配置管理地址 1.1.1.101/24。

图1-19 配置设备 B 的管理地址

5. 验证配置

(1) 通过管理地址 1.1.1.100/24 访问设备 A，查看 HA 监控页面。

图1-20 设备 A 的 HA 监控页面显示

(2) 通过管理地址 1.1.1.101/24 访问设备 B，查看 HA 监控页面。

图1-21 设备 B 的 HA 监控页面显示

目 录

1 接口状态同步组 ·····1-1
1.1 概述 ·····1-1
1.2 接口状态同步组 ·····1-1
1.3 接口状态同步组配置 ·····1-2

1 接口状态同步组

1.1 概述

接口状态同步组，即是为加快链路状态变化的快速响应而出现的一种高可靠的功能。主要功能是将一个组内的多个接口状态保持同步，即组内的某一成员状态首先发生变化，则组内的其它成员也同时被置为与其一致的状态，只有当该成员状态恢复时，其它组内成员的状态才可以恢复。

1.2 接口状态同步组

通过菜单“系统管理 > 系统设定 > 高可用性 > 接口状态同步组”，进入如图 1-1 所示页面。在该页面上，可以查看和编辑已经配置的接口状态同步组。详细信息说明如表 1-1 所示。

图1-1 接口状态同步组

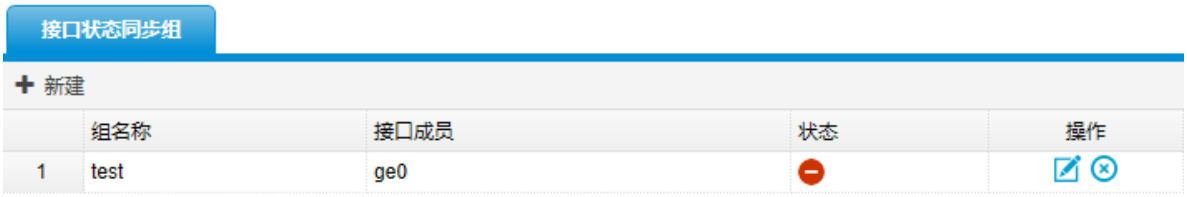


表1-1 接口状态同步组的显示信息

标题项	说明
组名称	接口状态同步组名称。
接口成员	同步组内成员。
状态	表示组状态为up，表示组状态为down • 组状态 分为 up，down 和 unknow 三种状态； • 组状态的确定： • 当全部成员的链路状态都为 up 时，组状态为 up； • 当某一成员的链路状态为 down 时，组状态为 down； • 当条件 2 中有成员的链路状态变为 up 时，将组内其它成员置为管理 up，组状态置为 unknow； • 当组状态为 unknow 时，继续调用 1、2 操作； • unknow 状态为中间状态，为防止组内成员间的互相影响，所以当组状态为 unknow 时，需要下一轮循环更新组状态。
操作	点击可以对该配置进行修改，点击可以删除该条配置。

1.3 接口状态同步组配置

通过点击图 1-1 中的“新建”，进入如图 1-2 所示页面。各配置项含义如表 1-2 所示。

图1-2 接口状态同步组配置页面

表1-2 接口状态同步组配置项含义

标题项	说明
组名称	设置接口状态同步组的名称
接口成员	左侧为设备上现有的接口列表，右侧为已经加入该同步组的接口列表

说明

- 接口状态同步组中，最多可以配置 8 个物理接口。
- 一个物理接口只能属于一个接口状态同步组。
- 设备支持的接口状态同步组的最大个数为 16。

目 录

1 地址探测 ····· 1-1
1.1 概述 ····· 1-1
1.1.1 地址探测简介 ····· 1-1
1.1.2 基于接口探测 ····· 1-1
1.1.3 可以在 HA 备设备使用路由探测 ····· 1-1
1.1.4 地址探测组 ····· 1-1
1.2 地址探测和其它模块的联动 ····· 1-1
1.3 配置地址探测 ····· 1-2
1.3.1 配置概述 ····· 1-2
1.3.2 地址探测配置 ····· 1-2
1.3.3 地址探测组配置 ····· 1-5
1.4 配置接口状态探测 ····· 1-6
1.4.1 接口状态探测配置 ····· 1-6
1.5 配置举例 ····· 1-8
1.5.1 接口状态探测配置举例 ····· 1-8

1 地址探测

1.1 概述

1.1.1 地址探测简介

使用 ICMP 协议，TCP 协议和 DNS 协议确定地址是否可达，从而实现判断链路状态。

1.1.2 基于接口探测

配置过程中可以指定探测报文的发送接口，也可以不指定具体接口，根据路由选路。指定接口主要用于和路由联动的情况。防止由于正常的链路失效后，备份路由启用，探测报文选择了备份路由接口，错误的认为探测地址可达的情况。

1.1.3 可以在 HA 备设备使用路由探测

HA 备设备只允许源地址为管理地址的报文发送，所以备设备发送探测报文的源地址为接口的管理地址。

注意

如果 HA 的备设备需要使用地址探测，必须在出接口上配置 HA 管理地址，否则无法发送探测报文。

1.1.4 地址探测组

可以将多个地址探测条目加入一个地址探测组中，地址探测组可以根据组内探测条目的结果，判断地址探测组的状态。探测组可以配置严格模式或者非严格模式。严格模式中，地址组内所有的探测条目都成功，探测组的状态才是成功的。非严格模式中，只要探测组中有一个探测条目成功，探测组的状态说就是成功的。

1.2 地址探测和其它模块的联动

- 和路由等模块联动，可以根据探测结果，禁用和启用某条路由。详见静态路由配置等。
- 和接口状态联动，可以根据探测结果，开启和关闭接口，以便通知下游设备。
- 和 HA 联动，HA 可以根据探测结果，判断网络状态。如果主设备地址探测结果失败，将切换成备设备。如果备设备的地址探测结果成功，并且配置了抢占为主，也可以抢占成主设备。详见 HA 配置。

注意

- 配置文件全部读取完成后，如果配置 HA，HA 的状态不再是 init 状态后。地址探测才能开始发包和计算超时。
- 如果路由和状态为初始化的地址探测联动时，路由暂定为有效，直到地址探测失败，才将路由置为无效。
- HA 和状态为初始化的地址探测联动，暂时不改变 HA 状态，直到地址探测成功或者地址探测失败，再通知到 HA 修改状态。
- 和地址探测联动的路由，当地址探测失败时，不可以被其它报文的转发使用，但是可以被地址探测的报文使用。比如配置默认路由和地址探测联动，当地址探测失败时，非探测报文不可以使用默认路由转发，但是地址探测报文依然可以使用默认路由转发。

1.3 配置地址探测

1.3.1 配置概述

地址探测配置的推荐步骤如表 1-1 所示。

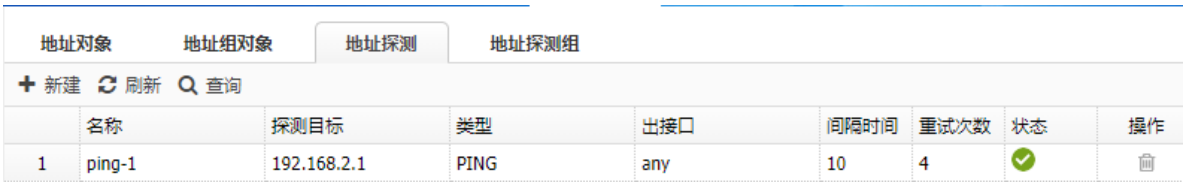
表1-1 地址探测配置的推荐步骤

配置任务	说明	详细配置
配置地址探测	必选	1.3.2
配置地址探测组	可选	1.3.3

1.3.2 地址探测配置

在导航栏中选择“策略配置 > 对象管理 > 地址对象”，点击上方“地址探测”标签进入地址探测显示页面，如图 1-1 所示。

图1-1 地址探测显示页面



页面的详细说明如表 1-2。

表1-2 地址探测显示的详细说明

项目	说明
名称	地址探测的名称。
探测目标	地址探测的目标，可以使IP地址，也可以是域名。
类型	地址探测的类型，有PING，TCP和DNS三种。
出接口	地址探测报文的出接口。
间隔时间	地址探测报文发送时间间隔。
重试次数	在地址探测失败之前可以发送的探测报文个数。
状态	地址探测的状态， 表示探测成功， 表示探测失败。
操作	可以执行删除操作。

点击右侧的删除按钮，可以删除对应的地址探测。

点击<新建>按钮，可以进入地址探测配置页面，如图 1-2 所示。

图1-2 地址探测配置页面

如果在类型中选中 TCP，页面中还会弹出 TCP 端口输入框，如图 1-3。

图1-3 TCP 地址探测配置页面

页面的详细说明如图 1-3 示。

表1-3 地址探测配置页面详细说明

项目	说明
名称	地址探测的名称。
探测目标	地址探测的目标，可以使IP地址，也可以是域名。
类型	地址探测的类型，有PING，TCP和DNS三种。
端口	TCP探测的目标端口。
出接口	地址探测报文的出接口。
间隔时间	地址探测报文发送时间间隔。
重试次数	在地址探测失败之前可以发送的探测报文个数。

输入完毕后，点击<提交>按钮，应用配置。

注意

- 已经被配置为地址探测出接口的接口不能配置和地址探测联动。
- 子接口已经被配置为地址探测出接口的接口不能配置和地址探测联动。
- 已经配置了和地址探测联动的接口不能作为地址探测的出接口。
- 已经配置了和地址探测联动的接口的子接口不能作为地址探测出接口。

1.3.3 地址探测组配置

在导航栏中选择“策略配置 > 对象管理 > 地址对象”，点击上方“地址探测组”标签进入地址探测组显示页面，如图 1-4 所示。

图1-4 地址探测组显示页面

页面的详细说明如表 1-4。

表1-4 地址探测组显示页面详细说明

项目	说明
名称	地址探测组的名称。
成员	地址探测组的成员。
模式	地址探测组的模式，有严格模式和非严格模式两种。
描述	地址探测组的描述。
状态	地址探测组的状态 表示探测成功， 表示探测失败。
操作	可以对地址探测组执行的操作。

点击页面左上方的<新建>钮者地址探测组右侧的<编辑>按钮，可以进入地址探测组的配置页面,如图 1-5。

图1-5 地址探测组编辑页面

地址探测组页面的详细描述如表 1-5。

表1-5 地址探测组配置页面详细描述

项目	说明
名称	地址探测组的名称。
描述	地址探测组的描述。
模式	地址探测组的模式，选中复选框表示严格模式，不选中是非严格模式，缺省是非严格模式。
已选成员	目前已经选中的地址探测组的成员。
名称	可以加入探测组的地址探测的名称。
探测目标	地址探测的目标。
状态	地址探测的状态 表示已经探测成功， 表示探测失败。

输入完毕后，点击<提交>按钮，应用配置。

说明

一个地址探测组中最多只能加入 10 个地址探测成员。

1.4 配置接口状态探测

1.4.1 接口状态探测配置

在导航栏中选择“系统管理 > 高可用性 > 接口状态探测”，进入接口状态探测显示页面，如图 1-6 所示。

图1-6 接口状态探测显示页面

页面的详细说明如表 1-6。

表1-6 地址探测显示的详细说明

项目	说明
监控接口	状态探测的接口。
地址探测	和接口联动的地址探测或地址探测组。
状态	地址探测或地址探测组的状态， 表示探测成功， 表示探测失败。
操作	可以执行删除操作。

说明

这里的状态指和接口联动的地址探测或者地址探测组状态，而不是接口的当前物理状态。

点击右侧的删除按钮，可以删除对应的接口状态探测。

点击<新建>按钮，可以进入接口状态探测配置页面，如图 1-7 所示。

图1-7 接口状态探测配置页面

页面的详细说明如表 1-7。

表1-7 接口状态探测页面详细说明

项目	说明
监控接口	状态探测的接口。
地址探测	和接口联动的地址探测或地址探测组。

输入完毕后，点击<提交>按钮，应用配置。

注意

- 已经被配置为地址探测出接口的接口不能配置和地址探测联动。
- 子接口已经被配置为地址探测出接口的接口不能配置和地址探测联动。
- 已经配置了和地址探测联动的接口不能作为地址探测的出接口。
- 已经配置了和地址探测联动的接口的子接口不能作为地址探测出接口。

1.5 配置举例

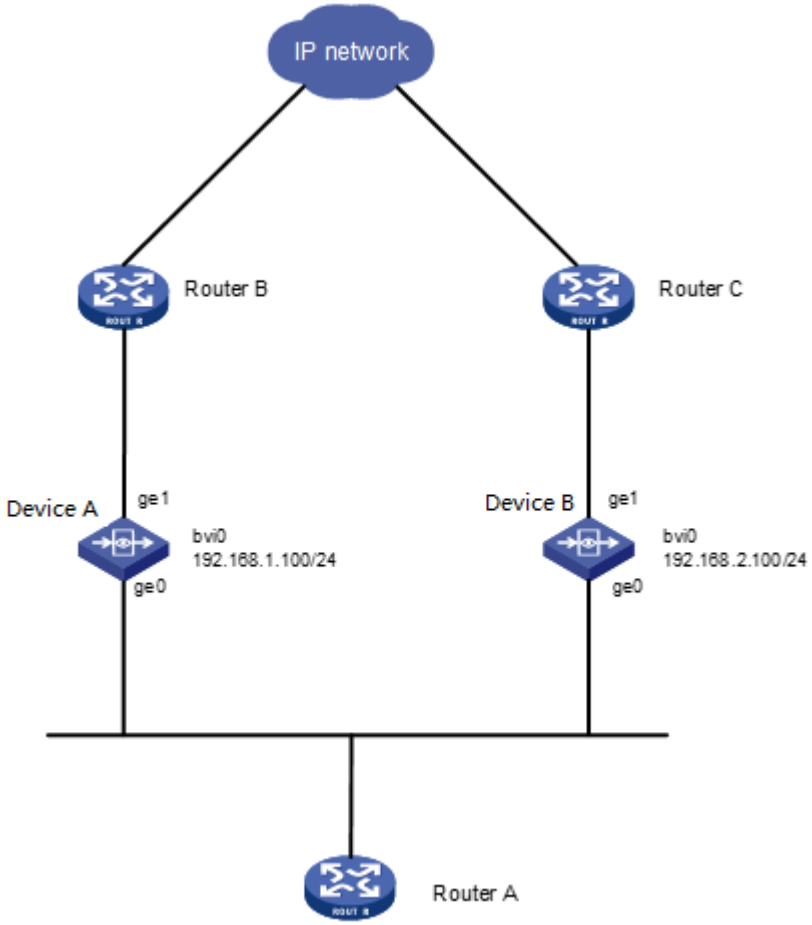
1.5.1 接口状态探测配置举例

1. 组网需求

- 两台设备使用透明模式和两台网关 Router B，Router C 以及核心路由器 Router A 相连。
- 设备 A 和设备 B 在桥上配置 IP 地址，并且都可以访问 Internet。

2. 组网图

图1-8 接口状态配置组网图



3. 配置思路

- 设备通过各自连接网关探测 Internet 上的服务器，检查网关是否正常。
- 当网关发生错误，无法连接 Internet 时，被设备发现，关闭和 Router A 相连的接口，促使 Router A 改变路由选路，从另外一侧发送数据。

4. 配置步骤

(1) 桥接口配置 IP 地址

图1-9 设备 A 的桥接口配置

图1-10 设备 B 的桥接口配置

(2) 配置地址探测

图1-11 设备 A 和设备 B 的地址探测配置

(3) 配置接口状态探测

图1-12 设备 A 和设备 B 的接口状态探测

5. 验证配置

(1) 查看设备 A 和设备 B 的接口状态探测显示页面

图1-13 设备 A 和设备 B 的接口状态显示页面

目 录

1 Portal 逃生 ·····1-1
1.1 Portal 逃生介绍 ·····1-1
1.2 Portal 逃生的配置 ·····1-1
1.3 配置举例 ·····1-2
1.3.1 Portal 逃生的配置举例 ·····1-2

1 Portal 逃生

1.1 Portal逃生介绍

Portal 逃生：当发生网络问题导致 Portal 服务器不可用时，对于指定用户无需认证仍可上网。

已认证用户：包含设备启动后新认证的在线用户和设备启动前曾经认证过的未在线用户。

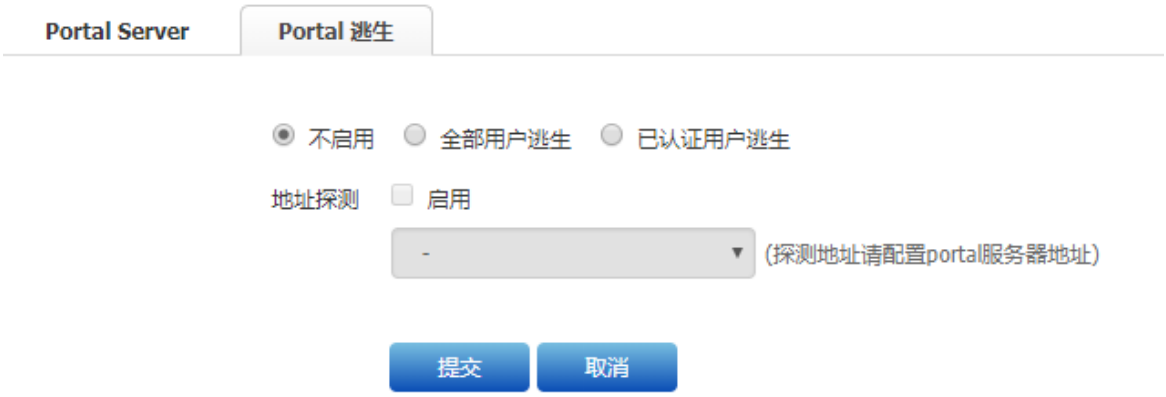
全局逃生模式：开始逃生时，所有用户均可上网。

已认证用户逃生模式：开始逃生时，只有已认证用户才可上网。

1.2 Portal逃生的配置

通过菜单“用户管理>认证管理>认证方式>portal server>portal 逃生”，进入如图 1-1 所示的页面。在该页面上，可以开启 portal 逃生的功能。

图1-1 开启 portal 逃生功能



选择“地址探测对象”，进入如图 1-2 所示的 portal 逃生的配置页面，各个配置项的含义如表 1-1 所示。

图1-2 Portal 逃生选择地址探测对象

表1-1 Portal 逃生的配置项含义

标题项	说明
不启用	关闭portal功能。
全部用户逃生	开始逃生时，所有用户均可上网。
已认证用户逃生	开始逃生时，只有已认证用户才可上网。
地址探测	探测地址，如果地址探测失败，portal逃生功能开启。

说明

- 已认证用户逃生，包含设备启动后新认证的在线用户和设备启动前曾经认证过的未在线用户。
- 对于全局逃生模式，要求在逃生时所有用户均可上网、逃生结束后未认证用户均需认证。也就意味着，在逃生期间在线用户不发生变动。
- 1G 内存设备存储规格为 1000。
- 2G 内存设备存储规格为 5000。
- 4G 内存设备（含小于 8G 设备）存储规格为 1W。
- 8G 及超 8G 内存设备规格为 2W。

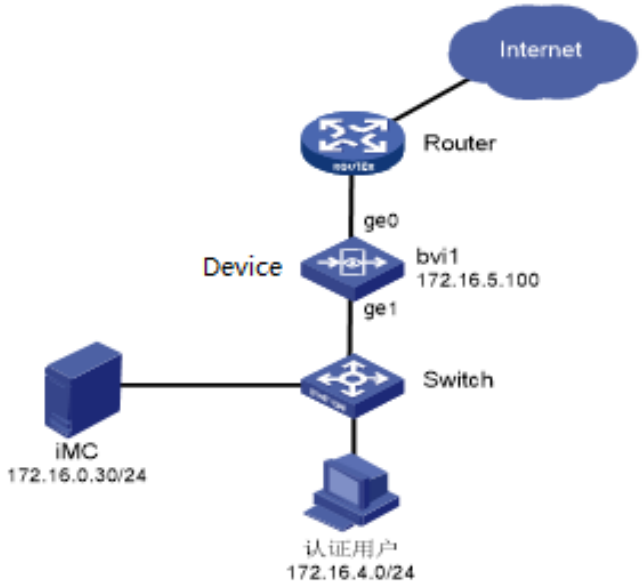
1.3 配置举例

1.3.1 Portal 逃生的配置举例

1. 组网需求

各设备接口及主机的 IP 地址和掩码如图 1-3 所示。认证用户通过设备设备正常上网

图1-3 Portal 逃生的配置案例组网图



2. 配置步骤

(1) 如图 1-4，在设备上配置 iMC 对应的 Radius 服务器。

图1-4 配置 Radius 服务器

(2) 如图 1-5，在设备上配置 iMC 对应的 Portal 服务器

图1-5 配置 Portal 服务器

(3) 如图 1-6，在设备上配置地址对象，注意在认证目的地址中排除 iMC 服务器地址 172.16.0.30

图1-6 配置排除 iMC 服务器地址和 172.16.0.30

(4) 如图 1-7，在设备上配置 portal 认证用户策略

图1-7 配置 portal 认证用户策略

(5) 如图 1-8，设备配置地址探测

图1-8 地址探测

(6) 如图 1-9，开启 portal 逃生功能，选择已认证用户逃生模式，添加地址探测。

图1-9 开启 portal 逃生功能

(7) 手动关闭 portal 服务器，查看设备已经认证的服务器是否能正常上网，查看从未认证过的设备的用户是否能正常上网。

3. 验证配置

查看当 portal 逃生的地址探测失败情况下，已经认证的用户能够正常上网，从未认证过的用户无法正常上网，如图 1-10。

图1-10 地址探测状态为 down，设备 portal 逃生功能开始生效

通过命令行查看设备存储的已认证用户。当 portal 逃生生效的时候，如果选择已认证用户逃生，包含设备启动后新认证的在线用户和设备启动前曾经认证过的未在线用户均可以正常上网。

#查看设备存储的已认证用户

```
HOST# display user-authed
#max number can save:1000
#user-authed count:1
user            mac                    online time          alive time              login
times
zhangsan     00:00:00:00:00:01  2020/09/06 21:21   2020/09/06 21:21   4
```

目 录

1 无线非经 ····· 1-1
1.1 简介 ····· 1-1
1.2 无线非经配置 ····· 1-1
1.2.1 配置厂商 ····· 1-1
1.2.2 配置场所 ····· 1-4
1.2.3 配置 AP ····· 1-8
1.2.4 配置上报周期 ····· 1-10
1.2.5 配置应用关系对照表 ····· 1-12
1.3 日志查询 ····· 1-13
1.3.1 终端上下线日志 ····· 1-13
1.3.2 虚拟身份日志 ····· 1-14
1.3.3 上网日志 ····· 1-15
1.3.4 普通内容日志 ····· 1-16

1 无线非经

1.1 简介

无线非经即公共场所无线上网安全管理条例，非经营性互联网信息服务提供者从事非经营性互联网信息服务时，应当遵守国家的有关规定，接受有关部门依法实施的监督管理。

无线非经功能配置主要包括厂商、场所、AP、上报周期、应用关系对照表五个方面的配置，具体如下：

- 厂商：隶属有关部门授权并遵循指定的标准（协议、应用维度）和一定的行为规则（场所编码规则、经营性质等），对外提供开放接口用来收集指定场所用户上网行为数据平台。
- 场所:经过设备的流量是从哪些场所过来,就填写哪些场所,表明有多少个场所流量经过设备。
- AP：AP 是存在于场所内的，表明该场所内有多少个 AP；这样可以知道具体某个用户是在哪一个场所中的哪一个 AP 使用网络。
- 上报周期：根据对接厂商标准接口文档按一定的周期上报无线非经数据。
- 应用关系对照表：按照对接厂商平台要求，将我司应用转换成其对应的应用 ID 上报至网监平台，以便网监平台显示对应应用名称。

无线非经功能主要目的是将对接厂商需要的数据按照一定的格式要求，采用指定的协议标准上传至网监平台服务器，实现网监对非经营性场所上网用户行为的监控。

1.2 无线非经配置

1.2.1 配置厂商

在导航栏中选择“系统管理>系统设定>无线非经>厂商配置”，进入厂商配置页面，在该页面上可以选择相关对接厂商配置相关数据，如图 1-1 所示；厂商配置页面展示详细说明如表 1-1 所示。

图1-1 厂商配置页面

表1-1 厂商配置页面详细说明

标题项	说明
对接厂商	当前要对接的网监平台。
对接地区	设备部署区域，如果设备无硬盘，则对接地区显示为空。
对接文档版本	用于区分同一对接网监平台的不同对接文档版本
名称	厂商名称。
组织机构代码	厂商组织机构代码。
社会信用代码	终端安全厂商统一社会信用代码
地址	厂商地址。
姓名	厂商负责人。
电话	厂商联系人方式。
邮件	厂商联系人邮箱。

标题项	说明
对接协议	网监平台提供厂商上报数据传输文件的协议（目前主要有FTP、SFTP、TCP/UDP方式）。
服务器地址	对接网监平台提供厂商上报数据的服务器地址。
服务器端口	对接网监平台提供厂商上报数据的服务器端口。
服务器用户名	对接网监平台提供厂商上报数据的用户名。
服务器密码	对接网监平台提供给厂商上报数据的密码。

以对接厂商选择任子行为例，配置完相关参数，点击“提交”按钮，则厂商添加完成，如图 1-2 所示。

图1-2 任子行网监平台对接厂商配置页面

1.2.2 配置场所

在导航栏中选择“系统管理>系统设定>无线非经>场所配置”，进入场所配置的显示页面，如图 1-3 所示；场所配置页面各项参数说明如表 1-2 所示。

图1-3 场所配置页面

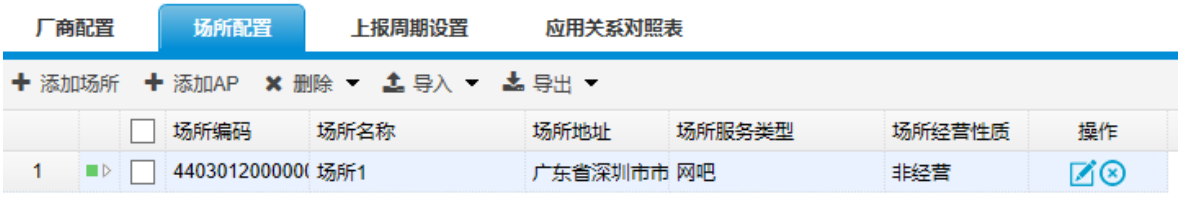
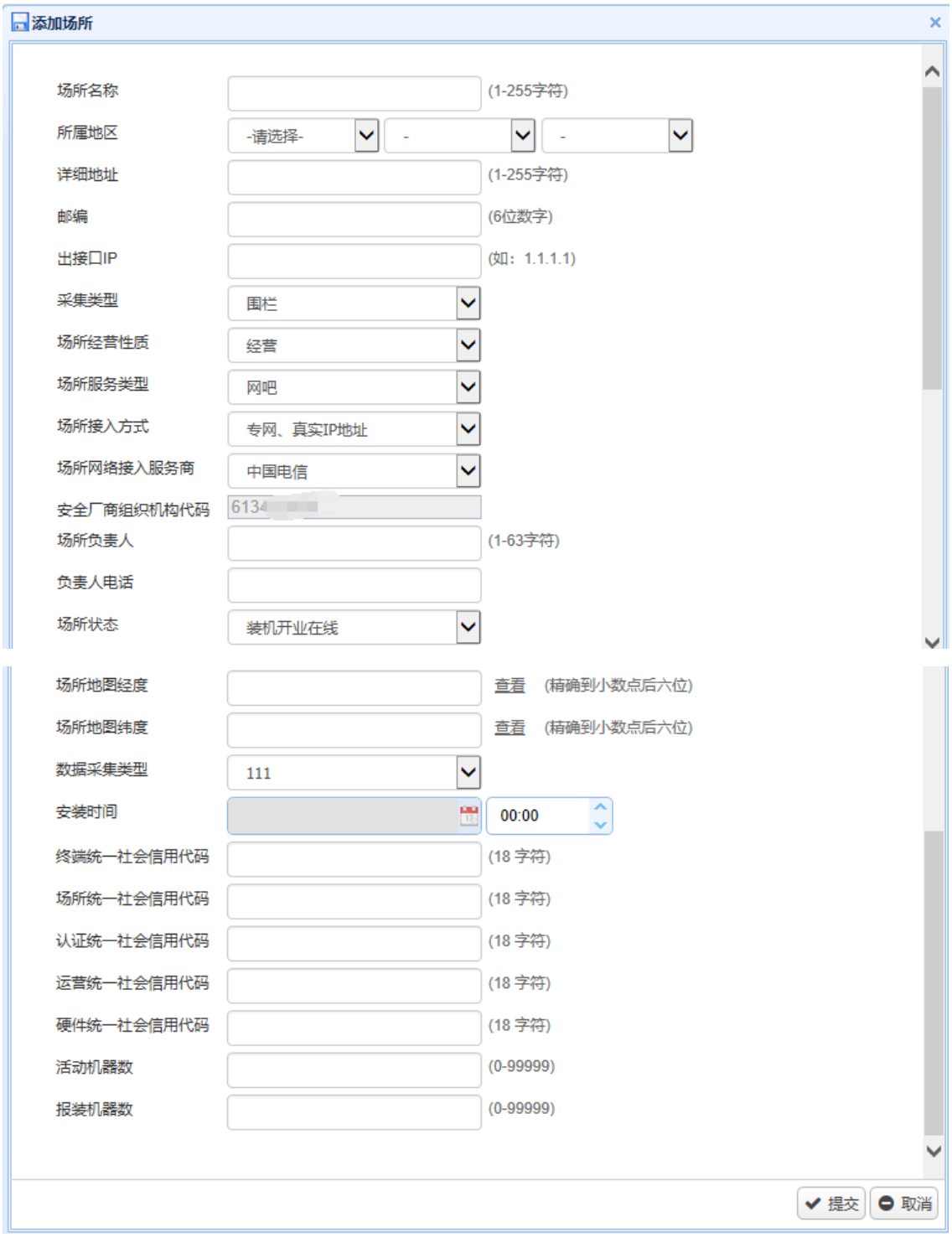


表1-2 场所配置页面的详细说明

标题项	说明
添加场所	点击该按钮进行场所添加。
添加AP	点击该按钮进行AP添加，但AP添加必须要先选中一个场所，才能添加对应的AP。
删除	选项需要删除的场所或AP进行删除，如果场所下有AP，不能直接删除场所，需要优先删除AP。
导入	可以分别对场所、AP进行单独的导入，场所、AP数据支持以csv格式导入。
导出	可以分别对场所、AP进行单独的导出，场所、AP数据支持以csv格式导出。
场所编码	上网服务场所包括经营性上网服务场所和非经营性上网服务场所，编码由14位阿拉伯数字组成，编码规则需要根据网监平台提供的对接文档要求进行显示。
场所名称	上网服务场所名称。
场所地址	上网服务场所详细地址。
场所服务类型	上网服务类场所类型（如旅店宾馆类、公共服务场所等，根据网监平台提供的对接文档可以查询详细的场所服务类型）。
场所经营性质	场所经营性质主要有经营、非经营、其它等，不同网监平台对接的场所经营性质代码不一样，需要参考对接文档。
操作	对已配置的场所可进行编辑、删除操作。

单击“添加场所”按钮，进入添加场所页面，如图 1-4 所示。

图1-4 添加场所页面



添加场所页面的详细说明如表 1-3 所示。

表1-3 添加场所配置的详细说明

标题项	说明
场所名称	上网服务场所名称。

标题项	说明
所属地区	上网服务场所地址区域。
详细地址	上网服务场所详细地址。
邮编	上网服务场所邮政编码。
出口IP	上网服务场所设备出口IP地址。
采集类型	场所数据采集类型（围栏、wifi、车载、其它）。
场所经营性质	场所经营性质主要有经营、非经营、其它等，不同网监平台对接的场所经营性质代码不一样，需要参考对接文档。
上网服务场所编码	上网服务场所包括经营性上网服务场所和非经营性上网服务场所，编码由14位阿拉伯数字组成，编码规则需要根据网监平台提供的对接文档要求进行显示。
场所服务类型	上网服务类场所类型（如旅店宾馆类、公共服务场所等，根据网监平台提供的对接文档可以查询详细的场所服务类型）。
场所接入方式	上网服务场所接入网络的方式（ADSL拨号、专线等）。
场所网络接入服务商	上网服务场所接入的网络运营服务商（中国电信、中国移动、中国联通等）。
安全厂商组织机构代码	场所与厂商通过组织机构代码进行关联使用。
场所负责人	上网服务场所负责人姓名。
负责人电话	上网服务场所负责人电话。
场所状态	上网服务场所安装营业状态（装机开业在线、装机开业离线、勒令停业等），对接网监平台文档中有相应的文档说明。
场所地图经度	上网服务场所部署位置的经度、点击“查看”按钮，搜索当前场所，会显示当前场所在地图的经度。
场所地图纬度	上网服务场所部署位置的纬度、点击查看按钮，搜索当前场所，会显示当前场所在地图的纬度。
数据采集	上网服务场所数据采集类型（如IDC、网吧、学校及培训中心等），对接网监平台文档中有相应的文档说明。
安装时间	上网服务场所设备的安装时间。
终端统一社会信用代码	终端安全厂商统一社会信用代码，具体参考对接文档。
场所统一社会信用代码	场所（如网吧、宾馆等）统一社会信用代码，具体参考对接文档。
认证统一社会信用代码	认证厂商统一社会信用代码，具体参考对接文档。
运营统一社会信用代码	运营厂商统一社会信用代码，具体参考对接文档。
硬件统一社会信用代码	安全设备硬件提供商统一社会信用代码，具体参考对接文档。
活动机器数	运行的设备数量。
报装机器数	准备安装的数量。

以对接厂商选择任子行为例，配置完相关参数，点击“提交”按钮，则场所添加完成，如图 1-5 所示。

图1-5 任子行网监平台对接场所配置页面

1.2.3 配置 AP

在导航栏中选择“系统管理>系统设定>无线非经>场所配置”，进入场所配置的显示页面，选择对应场所单击“添加 AP”按钮，进入添加 AP 页面，如图 1-6 所示；AP 配置页面各项参数说明如表 1-4 所示。

图1-6 添加 AP 页面

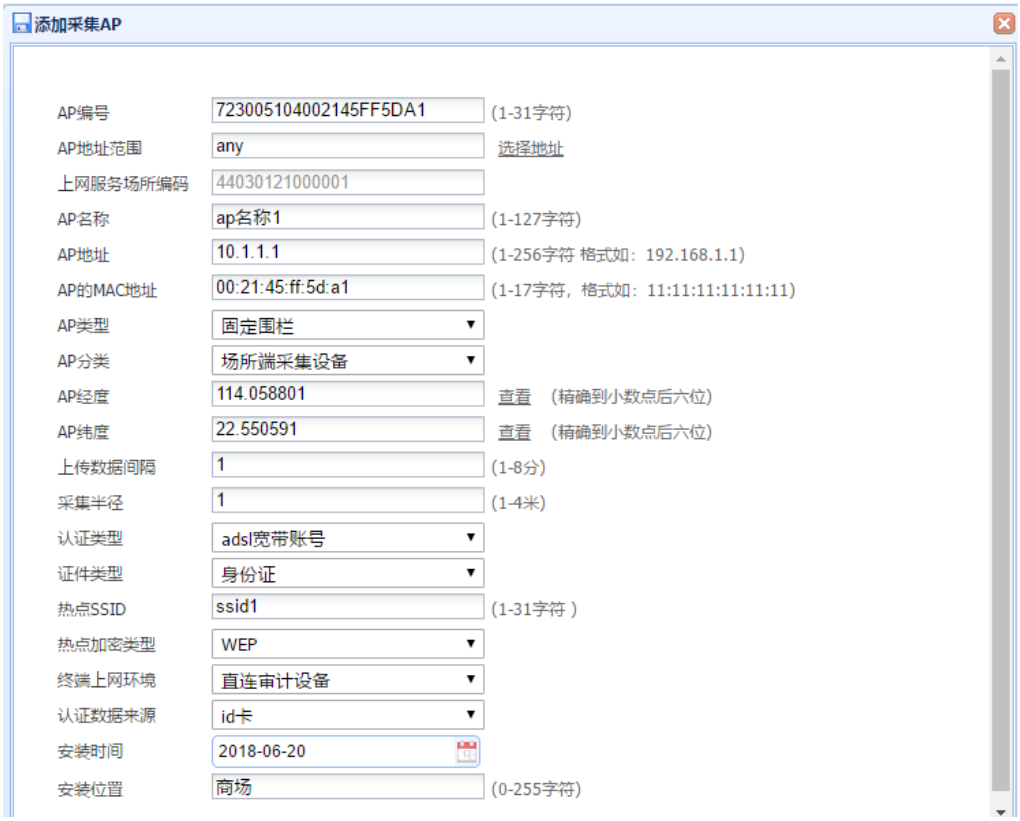
表1-4 添加 AP 配置的详细说明

标题项	说明
AP编号	AP编号是由21位字符组成唯一的编码，编号规则根据对接网监平台要求生成。
AP地址范围	AP的DHCP IP地址段范围。

标题项	说明
上网服务场所编码	AP所在场所的场所编码，AP必须挂在场所下，通过场所编码进行关联。
AP名称	AP设备配置名称。
AP地址	AP设备出口IP地址。
AP的MAC地址	AP设备出口MAC地址。
AP类型	AP设备类型（固定采集设备、移动车载采集设备、单兵采集设备、其它）。
AP分类	AP设备分类（场所端采集设备、围栏设备等）。
AP经度	AP设备部署位置的经度。
AP纬度	AP设备部署位置的纬度。
上传数据间隔	AP设备上传数据时间间隔。
采集半径	AP设备采集数据的半径范围。
认证类型	AP设备下用户的认证类型（adsl宽带账号、手机号等）。
证件类型	AP设备下用户使用的证件类型（如身份证、其它等）。
热点SSID	AP设备的热点SSID。
热点加密类型	AP设备设置热点使用的加密类型。
终端上网环境	终端上网环境，1 直连审计设备，2 通过非三层交换机等，具体参考对接文档。
认证数据来源	实名认证数据来源：0 ID卡，1手工输入 2 刷二代证等，具体参考对接文档。
安装时间	AP设备的安装时间。
安装位置	AP设备安装的位置。

以对接厂商选择任子行为例，配置完相关参数，点击“提交”按钮，则 AP 设备添加完成，如图 1-7 所示。

图1-7 任子行网监平台对接 AP 设备配置页面



1.2.4 配置上报周期

在导航栏中选择“系统管理>系统设定>无线非经>上报周期设置”，进入上报周期设置的显示页面，如图 1-8 所示，页面各个显示详细说明如表 1-5 所示。

图1-8 上报周期设置显示页面

表1-5 上报周期设置页面各个显示项说明表

标题项	说明
新建	新建上报日志策略。
删除	删除一个或多个上报日志策略。
状态	上报日志策略启用或禁用状态。

标题项	说明
名称	上报日志策略的名称。
脚本	上报日志策略的脚本。
执行周期	执行脚本的周期（单次、每周、每月）。
执行频率	执行脚本生成日志的频率。
每周	每周具体的上报周期及时间。
每月	每月具体的上报日期及时间。
操作	对已配置的上报日志策略可进行编辑、删除操作。

单击“新建”按钮，进入上报周期设置的配置页面，如图 1-9 所示，页面的详细说明如表 1-6 所示。

图1-9 新建上报周期

表1-6 页面详细说明

标题项	说明
启用	勾选“启用”后，才能进行策略配置 。
脚本名称	配置脚本的名称。
脚本类型	脚本类型跟配置的对接网监平台相关，此处无需配置，默认置灰。
脚本路径	选择需要上报的日志类型。
执行周期	选择执行脚本的周期单次、每周、每月。
执行频率	选择执行脚本生成日志的频率。

单击“提交”按钮，在上报周期设置页面，单击上报日志右侧“删除”按钮，可以删除对应的日志类型。

1.2.5 配置应用关系对照表

在导航栏中选择“系统管理>系统设定>无线非经>应用关系对照表”，进入应用关系对照表显示页面，页面中显示部分应用对照关系，如图 1-10 所示，页面显示详细说明如表 1-7 所示。

图1-10 应用关系对照表

		厂商	应用名	APP ID	关系对照ID	操作
1		任子行	股票登录_海通同花顺	2147483786	111111	
2		任子行	126邮箱	2147484449	1019023	
3		任子行	139邮箱	2147484450	1019044	
4		任子行	139邮箱(移动版)	2147485144	1019044	
5		任子行	163邮箱	2147484427	1019004	
6		任子行	189邮箱	2147484479	1019045	
7		任子行	21CN邮箱	2147484553	1019007	
8		任子行	263邮箱	2147485136	1019005	
9		任子行	58同城	2147484021	1429005	
10		任子行	58同城(Android版)	2147484140	1429005	
11		任子行	58同城(iOS版)	2147484141	1429005	
12		任子行	BING搜索(移动端)	2147484373	1250008	

表1-7 应用关系对照表显示页面详细说明

标题项	说明
新建	新建应用对照关系。
删除	删除一个或者多个应用对照关系。
导入	应用关系对照表支持以csv格式导入。
导出	应用关系对照表支持以csv格式导出。
查询	可按网监平台或应用名称进行查询。
厂商	对接的网监平台。
应用名	设备应用库中的应用名称 。
APP ID	设备应用库中应用对应的应用ID。
关系对照ID	网监平台提供的应用ID，需参考当前对接的网监平台文档中应用ID对照表填写。
操作	删除单个应用对照关系。

单击“新建”按钮，进入应用关系对照表的配置页面，如图 1-11 所示，页面显示详细说明如表 1-8 所示。

图1-11 新建应用关系对照表

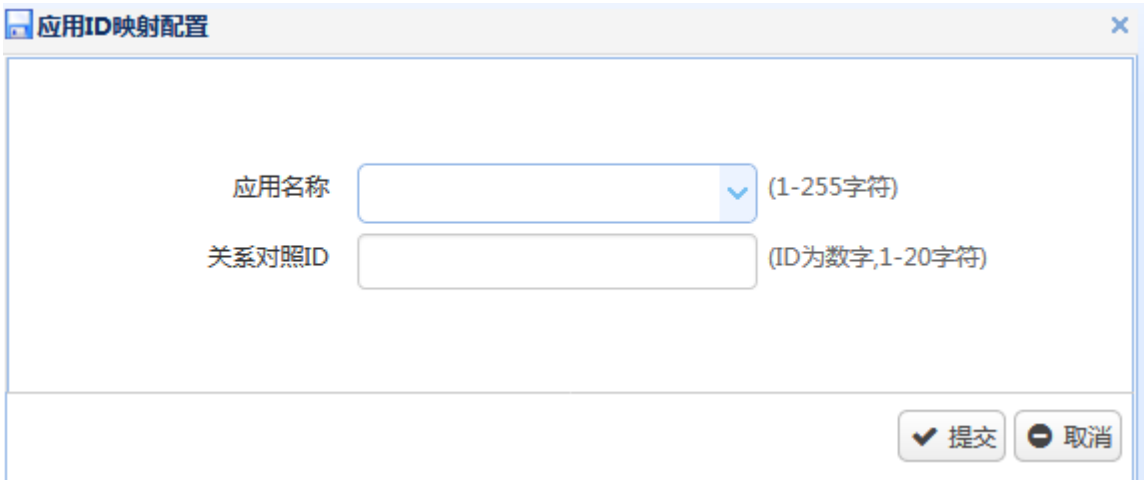


表1-8 页面详细说明

标题项	说明
应用名称	设备应用库中的应用名称 。
关系对照ID	网监平台提供的应用ID，需参考当前对接的网监平台文档中应用ID对照表填写。

1.3 日志查询

1.3.1 终端上下线日志

在导航栏中选择“系统管理>系统设定>无线非经>日志查询>终端上下线日志”，进入终端上下线日志显示页面，在该页面可以查看终端上下线日志信息，如图 1-12 所示，页面详细说明如表 1-9 所示。

图1-12 终端上下线日志

表1-9 终端上下线日志页面的详细说明

标题项	说明
查询	根据指定条件进行查询。

标题项	说明
重置	清除已支持的查询条件。
用户	认证用户账号。
用户MAC	认证用户对应的终端MAC地址。
IP地址	认证用户对应的终端IP地址。
认证类型	与AP页面上配置的认证类型有关。
行为	认证用户的状态（1表示上线、0表示下线）。
场所	该日志产生关联的场所名称。
AP MAC	该日志产生所关联的APMAC。
上线时间	认证用户对应认证上线时间。
下线时间	认证用户对应认证下线时间。
时间	产生日志的记录时间。

1.3.2 虚拟身份日志

在导航栏中选择“系统管理>系统设定>无线非经>日志查询>虚拟身份日志”，进入虚拟身份日志显示页面，在该页面可以查看虚拟身份日志信息，如图 1-13 所示，页面详细说明如表 1-10 所示。

图1-13 虚拟身份日志

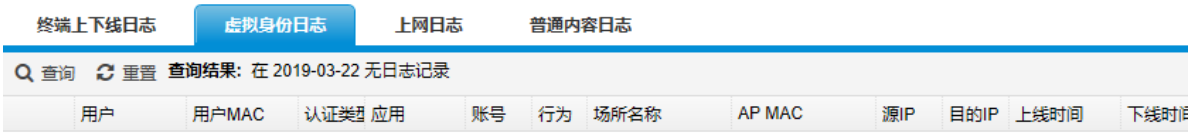


表1-10 虚拟身份日志页面的详细说明

标题项	说明
查询	根据指定条件进行查询。
重置	清除已支持的查询条件。
用户	认证用户账号。
用户MAC	认证用户对应的终端MAC地址。
认证类型	与AP页面上配置的认证类型有关。
应用	虚拟身份产生的具体应用。
账号	虚拟身份账号。
行为	虚拟身份的状态（1表示上线、0表示下线）。
场所名称	该日志产生所属的场所名称。

标题项	说明
AP MAC	该日志产生所属的AP MAC。
源IP	认证用户对应的终端IP地址。
目的IP	该用户访问具体应用对应的目的IP地址。
上线时间	该应用产生登录日志的时间。
下线时间	该应用对应真实身份数据下线的时间。
时间	设备端产生该日志的记录时间。

1.3.3 上网日志

在导航栏中选择“系统管理>系统设定>无线非经>日志查询>上网日志”，进入上网日志显示页面，在该页面可以查看上网日志信息，如图 1-14 所示，页面详细说明如表 1-11 所示。

图1-14 上网日志

表1-11 上网日志页面的详细说明

标题项	说明
查询	根据指定条件进行查询。
重置	清除已支持的查询条件。
用户	认证用户账号。
用户MAC	认证用户对应的终端MAC地址。
认证类型	与AP页面上配置的认证类型有关。
应用	虚拟身份产生的具体应用。
账号	虚拟身份账号，网页浏览应用此处填的也是URL信息。
名称	该日志产生所属的场所名称。
AP MAC	该日志产生所属的AP MAC。
URL	审计数据中对应应用产生的URL，通过app访问的有可能无法获取到URL，则此项有时为空。
源IP	认证用户对应的终端IP地址。
目的IP	该用户访问具体应用对应的目的IP地址。
时间	设备端产生该日志的记录时间。

1.3.4 普通内容日志

说明

普通内容日志页签，只有选择了特定的厂商后才会出现，比如任子行厂商。

在导航栏中选择“系统管理>系统设定>无线非经>日志查询>普通内容日志”，进入普通内容日志显示页面，在该页面可以查看普通内容日志信息，如图 1-15 所示，页面详细说明如表 1-12 所示。

图1-15 普通内容日志

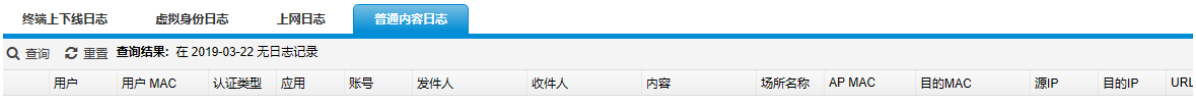


表1-12 上网日志页面的详细说明

标题项	说明
查询	根据指定条件进行查询。
重置	清除已支持的查询条件。
用户	认证用户账号。
用户MAC	认证用户对应的终端MAC地址。
认证类型	与AP页面上配置的认证类型有关。
应用	虚拟身份产生的具体应用。
账号	虚拟身份账号。
收件人	审计数据中的邮件收件人。
发件人	审计数据中的邮件发件人。
内容	审计数据中的如搜索关键字、发帖内容、邮件内容等。
场所	该日志产生所属的场所名称。
AP MAC	该日志产生所属的AP MAC。
源IP	认证用户对应的终端IP地址。
目的IP	该用户访问具体应用对应的目的IP地址。
URL	审计数据中对应应用产生的URL，通过app访问的有可能无法获取到URL，则此项有时为空。
时间	设备端产生该日志的记录时间。

目 录

1 告警功能 ····· 1-1
1.1 概述 ····· 1-1
1.2 告警功能配置 ····· 1-1
1.2.1 告警事件设置 ····· 1-1
1.2.2 邮件配置 ····· 1-3
1.2.3 邮件服务器设置 ····· 1-4
1.2.4 配置 DNS ····· 1-5
1.3 告警功能配置举例 ····· 1-6

1 告警功能

1.1 概述

当设备发生故障或某些原因导致系统发生不正常的工作或某些功能影响用户体验的情况下，系统可以根据不同类型的故障，并对故障进行分析并通过一定的告警方式通知用户或者网络管理员，这就是实现告警功能的目的。

为提高系统的实时监控能力，增加告警功能模块。该功能模块可以根据不同事件类型进行分析，分析结果以不同的告警方式通知用户或管理员。系统对以下产生的事件进行分析：

- 设备硬件事件，如 CPU 利用率过高、内存利用率过高等；
- 用户体验事件，如隧道断开等；
- 系统规格事件，如会话数目达到规格，接口流量超过阈值等。

1.2 告警功能配置

1.2.1 告警事件设置

在导航栏中选择“系统管理 > 系统维护 > 系统告警”，进入告警功能显示页面，页面显示了当前所有告警事件的类型，如图 1-1 所示。

图1-1 告警事件设置页面

表1-1 告警事件设置页面详细说明

项目	说明
启用事件告警	启用事件告警的全局按钮
CPU告警	可选开启CPU告警
阈值	可选CPU占用区间1%-100%
持续时长	CPU超过阈值持续时间

项目	说明
内存告警	可选开启内存告警
阈值	可选内存占用区间1%-100%
持续时长	内存超过阈值持续时间
硬盘告警	可选开启硬盘告警
阈值	可选硬盘占用区间1%-100%
持续时长	硬盘超过阈值持续时间
会话告警	可选开启会话告警
阈值	可选会话占用区间1%-100%
持续时长	会话超过阈值持续时间
整机流量告警	可选开启整机流量告警
阈值	整机流量占用区间10-10000Mbps
持续时长	整机流量超过阈值持续时间
IPsec-VPN连接断开告警	可选开启IPsec-VPN连接断开告警
移动终端管理告警	开启移动终端告警功能
LDAP服务器对接失败告警	开启/关闭LDAP服务器对接失败告警。
电源告警	勾选后，对于双电源的设备，如果有一个电源未接入会启用告警（仅支持双电源的设备）。

1.2.2 邮件配置

在导航栏中选择“系统管理 > 系统维护 > 系统告警 > 邮件配置”，页面显示了当前的邮件告警配置，如图 1-2 所示。

图1-2 邮件告警配置页面

页面的详细说明如表 1-2 所示。

表1-2 邮件配置详细说明

项目	说明
收件地址	收件地址
收件标题	收件标题
立即发送/间隔时间	发送邮件时间设置

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改，恢复至上一次配置。

1.2.3 邮件服务器设置

在邮件告警页面单击<邮件服务器设置>，进入邮件服务器配置页面，如图 1-3 所示。

图1-3 邮件服务器配置页面

页面的详细说明如表 1-3 所示。

表1-3 邮箱服务器配置详细说明

项目	说明
发件人地址	发件人邮箱地址
邮箱服务器	发送地址的邮箱服务器
服务器端口	服务器端口
SSL	选中后可设置SSL协议端口号
smtp 服务器身份验证	配置smtp 服务器身份验证的用户名、密码，如果不需要验证可不选。
测试邮箱有效性	检查配置是否正确，正确则会收到测试邮件

1.2.4 配置 DNS

在导航栏中选择“网络配置 > 基础网络 > DNS 服务”，进入 DNS 服务器的显示页面，如图 1-4 所示。

图1-4 DNS 服务器显示页面

页面的详细说明如表 1-4 所示。

表1-4 用户的详细说明

项目	说明
启用DNS代理	启用DNS开关。
DNS服务器1	DNS服务器1-4。

输入完毕后，点击<提交>按钮，应用配置，点击<取消>按钮，取消配置修改。

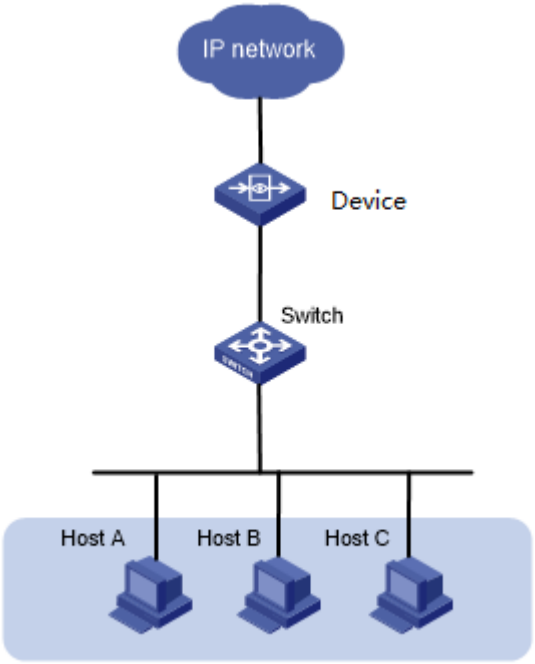
1.3 告警功能配置举例

1. 组网需求

设备 CPU、内存、整机流量使用超过阈值，设备产生告警日志。

2. 组网图

图1-5 组网图



3. 配置步骤

(1) 启用事件告警，设置 CPU 警告阈值为 50%，内存警告阈值为 10%，整机流量警告阈 10Mbps，所有的持续时长设置为 1 分钟。

图1-6 配置告警事件

(2) 配置邮件服务器。

图1-7 配置邮件服务器

(3) 配置 DNS

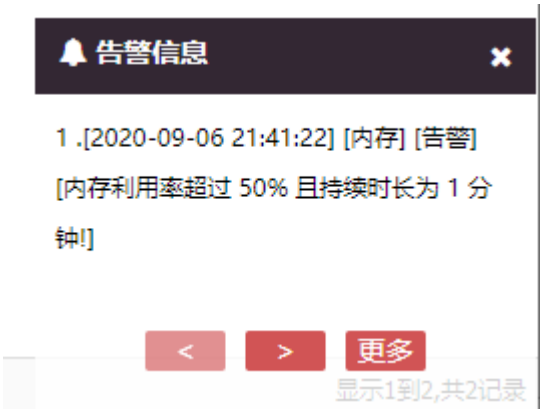
图1-8 配置 DNS 服务器

(4) 多主机流量过设备导致 CPU、内存、整机流量超过阈值，产生告警日志。

图1-9 产生告警日志

(5) 设备主页系统状态页面弹出告警窗。

图1-10 主页告警弹窗



(6) 邮箱接收告警日志邮件。

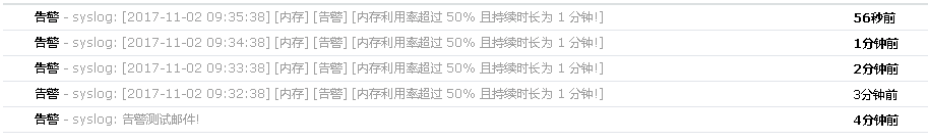



图1-11 邮件接收告警日志邮件