深信服行为管理AC

用户手册

适用版本：行为管理AC13.0.102

深信服科技股份有限公司

版权声明

特别提示

您购买的产品、服务或特性等应受深信服科技股份有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，深信服科技股份有限公司对本文档内容不做任何明示或默示的声明或保证。 由于产品版本升级或其他原因，本文档内容会不定期进行更新，如有变更，恕不另行通知。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保，深信服科技股份有限公司不对本文档中的遗漏、变更及错误所导致的损失和损害承担任何责任。

由于产品版本升级或其他原因，本文档内容会不定期进行更新，如有变更，恕不另行通知。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保，深信服科技股份有限公司不对本文档中的遗漏、变更及错误所导致的损失和损害承担任何责任。

联系我们

深信服技术支持网站： support.sangfor.com.cn
售前咨询热线：400-860-6868
售后服务热线：400-630-6430 （中国大陆）
深信服科技官方网站： www.sangfor.com.cn
7*24小时智能客服：
PC端：进入深信服社区首页（ bbs.sangfor.com.cn ）， 点击右侧 “智能客服”
移动端：手机扫描访问

打开微信扫一扫
可在手机端咨询

用户手册

产品概述

硬件平台

深信服全网行为管理AC(Access Control）采用软硬一体的网络设备产品形态，具有极高的稳定性与运行效率，方便部署于网络机房机架中。

• 高运行效率

全网行为管理系统产品全面采用先进的 X86 64bit 架构，配合 Intel 高性能处理器与芯片组，并且在全功能开启时依然保持极高的处理能力与运行效率。

• 硬件Bypass功能

硬件设计方面，AC 具有国际先进的硬件 Bypass 功能，能够在设备宕机、关机时，使每对网络接口自动保持连通，从而使设备的网络连通性不会受到影响。此外，AC全网行为管理系统 Bypass 功能支持主动开启，管理员可通过设备上的硬件 Bypass按钮或系统控制台的操作按钮进行开启或关闭。

软件系统

AC软件系统采用自主研发的高性能操作系统，并针对全网行为管理系统的各项功能进行了大量优化，从而在高负荷任务中依然保持着极强的可用性、稳定性与运行效率。

AC全网行为管理系统软件系统具有下列优势：

• 高可用性与稳定性

AC全网行为管理系统操作系统采用自主研发的Linux内核，使操作系统、底层功能核心、用户界面三者具有高度的耦合性，保证了系统的高可用性与稳定性。

• 一键搬包

AC全网行为管理系统的搬包功能可以在设备出现异常情况时提供紧急逃生能力，从而保证业务流量不中断，同时可快速定位故障点。搬包是一种更彻底的流量放通机制，搬包时CPU、内存、IO等资源占用将大幅降低。与直通、全局排除功能不同的是，搬包生效时所有数据包将会被直接转发，不会匹配任何策略逻辑，不会生成任何策略管控日志。

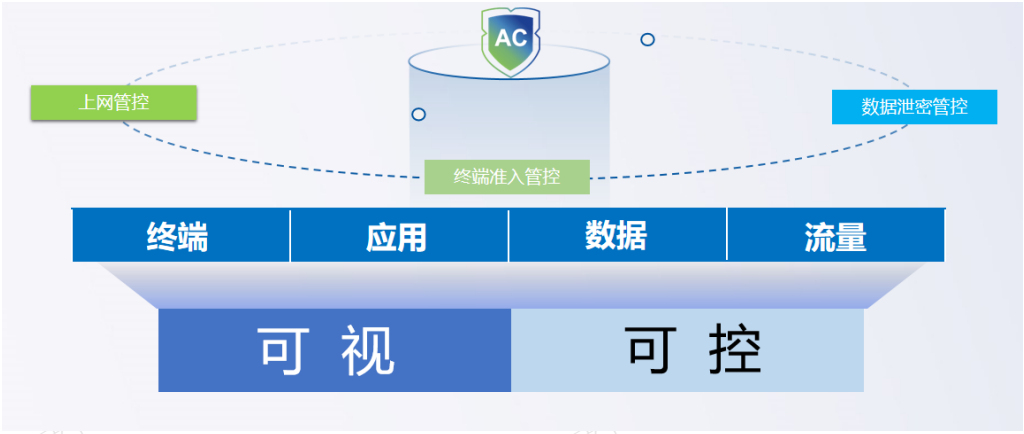
• 人性化操作

AC全网行为管理系统操作模式采用B/S架构，用户可利用浏览器登录AC全网行为管理系统管理平台。此外，全网行为管理系统在设计时就极为重视用户体验，在界面设计上采用了互联网领域先进的用户体验设计思想，例如功能模块的多标签化、审计结果的图表可视化等。

深信服全网行为管理广泛应用于政府、教育、金融、企业等办公网互联网出口（千兆和万兆）、有线无线混合网络出口、内网业务系统审计、上网行为审计、终端接入安全、内部威胁分析多分支组网、内网用户认证等场景，目前服务于5万多家各行业用户。

产品简介

全网行为管理AC实现对全网终端、应用、数据和流量的可视可控，智能感知终端违规接入、敏感数据泄密、上网违规行为等内部风险，解决上网管控、终端准入管控和数据泄密管控的场景问题，真正实现“内部风险智能感知，全网行为可视可控”的一体化管控。



产品特点

• 保障上网规范和上网体验，避免违法违规，减少上网抱怨。

• 建立终端入网安全规范，降低安全隐患和数据泄露风险。

• 建立数据外发规范，分析风险，防止敏感数据泄露。

产品关键特性

深信服全网行为管理，从入网、内部操作到出网整个流程，实现全局可视，闭环管控、智能感知，让行为更安全、更高效，其主要特性有：

• 扩大监控范围，实现用户深度管理

公司的IT管理员需要总概览公司内网全局网络分布使用的情况；查看终端设备的部署使用情况，IP分配情况，以及内网中网络设备（交换机、路由器、防火墙等）的分布使用情况，做到让管理员能时刻掌握网络资源分配和使用，实现了用户网络的深度管理。

• 加固终端安全，提升用户安全系数

AC终端安全能帮助用户实现对认证终端设备的全方位管理，具备了网关防病毒、终端安全级别检查等终端自身系统方面的策略。最新版本新增了外联检查功能，用于检查终端设备可能对网络安全带来威胁的多种外联行为；内网横向隔离的外联管控功能，可有效避免用户内部资料泄密，通过认证终端设备的外设接入管理规则，将威胁网络安全的不利因素拒之门外。

• 完善认证体系，提高入网管理力度

AC支持丰富的身份认证方式。为了提高用户的管理力度，提供了802.1x认证方式，802.1x是交换机端口授权的认证方式，能够在认证通过之前有效阻止PC的TCP和UDP报文，做到认证更保险，并且提供了认证失败的管理机制，可以让用户对认证有一个全面的把控。

• 扩展业务审计，实现网络全面管控

AC在互联网审计（应用审计、流量和上网时长审计、网页内容审计）、日志记录、报表分析等不同层级的全面业务审计，实现用户网络的全面管控，让用户对自己的内网有更多的管理监测方式。

• 优化流量管理，提升用户上网体验

AC能帮助管理者概览公司的带宽资源使用情况，可制定优化的带宽管理策略。该策略可以在工作时间保障核心用户、核心业务所需带宽，限制无关业务对资源的占用，也可以在带宽空闲时实现动态分配。为了实现资源的充分利用，在不同的时间段，不同的对象，不同的应用进行管道式流控，有效保障用户的上网体验，保障网络的稳定性。

• 管控网络应用，提高员工工作效率

AC数据中心能帮助组织管理者透彻了解员工的网络行为内容和行为分布情况。借助AC的管理功能，管理员

能实现分时间段、基于用户、基于应用、基于行为内容的网络行为控制，限制员工上班时间的无关网络行为，减少员工因效率低下带来的加班、离职、薪金浪费、额外薪金支出等问题。管理员使用AC数据中心可自定义“员工工作效率报表”，作为员工工作效率考核的辅助依据。

• 管控上网权限，实现职位与权限匹配

通过AC，管理员能依据组织架构建立用户身份认证体系，实现员工职位职责与上网权限的匹配。如限制研发部门不得使用webmail外发邮件；上班时间不能使用IM聊天工具，限制财务人员不能访问不受信网站等。以此减少越权访问和权限滥用的现象，防止泄密和不良舆论风险。

• 防范信息泄露，保障组织信息安全

互联网的普及让网络泄密和网络违法行为层出不穷，如果员工利用组织网络发生泄密或违法行为，且没有证据找到直接责任人，IT部门将成为该事件压力的承担者。通过AC，管理员能够实现基于内容的外发信息过滤，管控文件、邮件发送行为；对网络中的异常流量、用户异常行为及时发起告警；更有数据中心保留相关日志，风险智能报表发现潜在的泄密用户，实现“事前预防、事发拦截、事后追查”。

• 过滤不良信息，规避管理与法律风险

互联网资源极大丰富，亦良莠不齐。AC能帮助管理员过滤违法、违规不良网页，含有不良关键字的网络信息，防止用户不慎访问不受信的网站带来法律风险。对于内网用户的外发信息行为，AC基于内容的外发信息过滤能帮助管理员及时拦截不良言论，或者在特殊时期采用“允许看帖不允许发帖、允许收邮件不允许发邮件”的特殊管控手段，最大程度的减少舆论风险给组织形象声誉带来影响。

• 优化上网环境，提升上网安全

网络犯罪日益善用伪装。对于已中毒的终端，AC会检测网络中的异常流量如木马流量等并自动封锁并发起告警，提升局域网安全。

安装部署

本章主要讲解设备安装与升级过程中的流程、准备工作以及操作步骤等。

安装前准备

本节主要写作安装前的准备工作，包括准备工具、环境、软硬件材料要求等。

环境要求

深信服全网行为管理AC可在规范的环境下使用。为了保证系统能长期稳定的运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

表1AC环境说明

环境项	规范要求
电压	110V~230V
温度	0～45℃
湿度	5～90%
电源	交流110V到230V电源，接通电源之前，请保证您的电源有良好的接地措施。

产品外观

深信服全网行为管理AC前面板（以AC-1000-B1060为例）。

表2AC-1000-B1060 正面网口对照表

设备名称	序号（正面）	说明
AC-1000- B1060	1	USB接口
	2	CONSOLE口
	3	ETH0
	4	ETH1
	5	高可用性状态灯
	6	电源灯
	7	告警灯
	8	硬件型号

深信服全网行为管理AC背面板（以AC-1000-B1060为例）。

表3 AC-1000-B1060 背面网口对照表

设备名称	序号（背面）	说明
	1	设备信息

AC-1000- B1060	2	电源开关：1是开机；0是关机
	3	电源口

注意事项：

1. 告警灯在设备启动期间是红灯长亮的。通常一两分钟后红灯熄灭，说明正常启动。如红灯长时间不灭，请关闭设备等待5分钟后重新开机。
2. 如果还是长亮，请联系深信服科技客服确认是否设备损坏。正常启动后，有时红灯会闪烁，属于正常现象，红灯闪烁表示设备正在写系统日志。
3. 控制口仅供开发和测试调试使用。最终用户需从网口通过控制台接入。

配置与管理

在配置设备之前，需要配备一台电脑，并确保该电脑浏览器可以正常使用（如Internet Explorer、谷歌、火狐等主流的浏览器），然后把电脑与深信服全网行为管理AC连接在同一个局域网内，通过网络对设备进行配置。

单设备接线方式

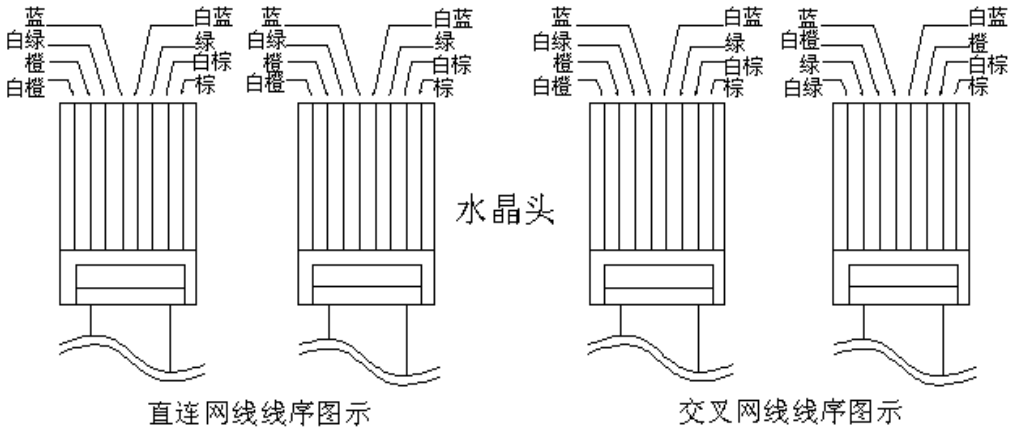
• 在背板上连接电源线，打开电源开关，此时前面板的Power灯（绿色，电源指示灯）和Alarm灯（红色，告警灯）会点亮。大约1-2分钟后Alarm灯熄灭，说明设备正常工作。

• 请用标准的RJ-45以太网线将ETH0（LAN）口与内部局域网电脑连接，对AC设备进行配置。

• 请用标准的RJ-45以太网线将ETH2（WAN1）口与Internet接入设备相连接，如路由器、光纤收发器或ADSL Modem等。

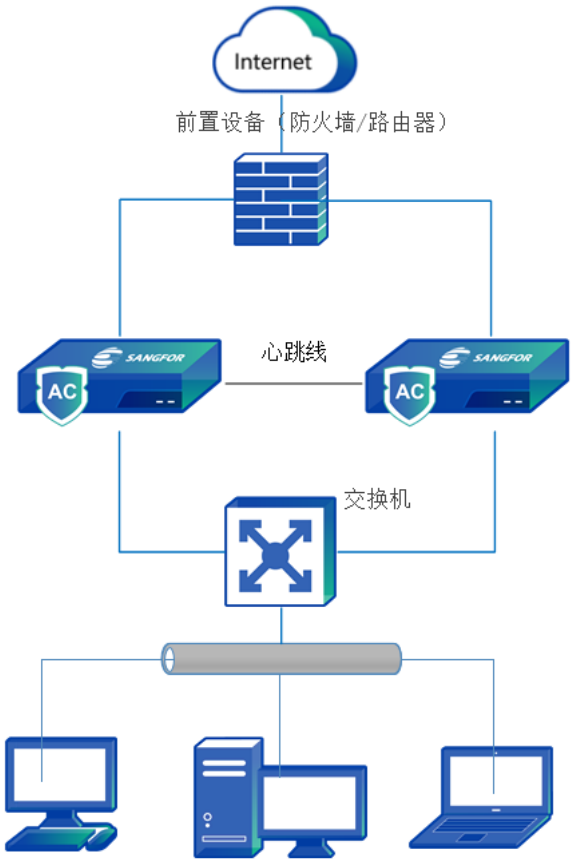
注意事项

1. 多线路的AC设备可以支持多条Internet线路，此时将WAN2口与第二条Internet接入设备相连，WAN3口与第三条Internet线路相连，依此类推。
2. 使用标准RJ-45以太网线将DMZ口与DMZ区的网络连接，DMZ区通常放置对外提供服务的WEB服务器、E-MAIL服务器等。AC设备可以为这些服务器提供安全保护。
3. 设备正常工作时POWER灯常亮，WAN口和LAN口LINK灯长亮，ACT灯在有数据流量时会不停闪烁。ALARM红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在安装时此红灯长亮，请将设备断电重启，重启之后若红灯一直长亮不能熄灭，请与我们联系。
4. WAN口直接连接MODEM应使用直连线、连接路由器应使用交叉线；LAN口连接交换机应使用直连线、直接连接电脑网口应使用交叉线。当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线顺序不同，如下图：



双机部署接线方式

若采用AC高可用的工作方式，按以下接线方式进行外网线路和内网线路的接线。



• 使用标准RJ-45以太网线将两台AC设备的ETH2（WAN1）口（若使用多线路技术，接线方式类似，保证两台设备的外网接口接到同一个外网线路即可）接到同一交换机上，再使用标准的RJ-45以太网线与Internet接入设备相连接，如路由器、光纤收发器或ADSL Modem等。

• 选一个空闲网口作为HA口，将两台AC设备的HA口用网线连接起来。

• 使用标准RJ-45以太网线将两台AC设备的ETH0（LAN）口接到同一交换机上，再使用标准的RJ-45以太网线与局域网交换机相连，连接到内部局域网。

• 接线完毕后，分别打开两台设备的电源，即可进行系统配置。双机系统配置时和单机系统配置一样，仅对一台主设备进行配置，另外一台从设备将自动进行同步，无需另行配置。

WEB控制台登录介绍

全网行为管理AC支持安全的HTTPS登录，是使用HTTPS协议的标准端口登录，为了防止配置过程中被截获而产生安全隐患。

深信服全网行为管理AC设备，各个网口默认的出厂IP为：

ETH0(LAN)：10.251.251.251/24，ETH1(DMZ)10.252.252.252/24。

• 如果电脑连接的是设备的ETH0口，需要线在电脑上配置一个10.251.251.0/24网段的地址，打开浏览器输入https://10.251.251.251登录设备网关控制台。

• 如果电脑连接的是设备的ETH1口，需先在电脑上配置一个10.252.252.0/24网段的地址，打开浏览器输入https://10.252.252.252 登录设备网关控制台。

操作步骤

步骤1.先在直连设备的计算机配置一个10.251.251.X网段的IP（如配置10.251.251.100），例如使用谷歌浏览器来访问，输入网址：https://10.251.251.251。出现一个如下图的安全提示，点击<高级>，然后再点击<继续前往>会跳转到控制台登录页面。

步骤2.在登录框输入用户名和密码，默认情况下用户名和密码均为：admin。阅读《用户协议&隐私政策》（若对此协议有疑问，请联系“深信服”沟通），勾选我已阅读并同意，点击<登录>按钮即可登录AC设备进行配置。

步骤3.当用户密码过于简单，则会被检测为弱密码，控制台会处理：登录后检查为弱密码，则会弹出告警提示。

步骤4.如果提示超过15天都没有修改密码，则会弹出强制修改密码提示。

步骤5.点击<立即修改>，可更改当前的密码。

部署模式

部署模式是用于设置设备的工作模式，可把设备设定为路由模式、网桥模式、旁路模式、单臂模式。选择一种合适的部署模式，是顺利将设备部署到网络中并且使其能正常运行的基础。

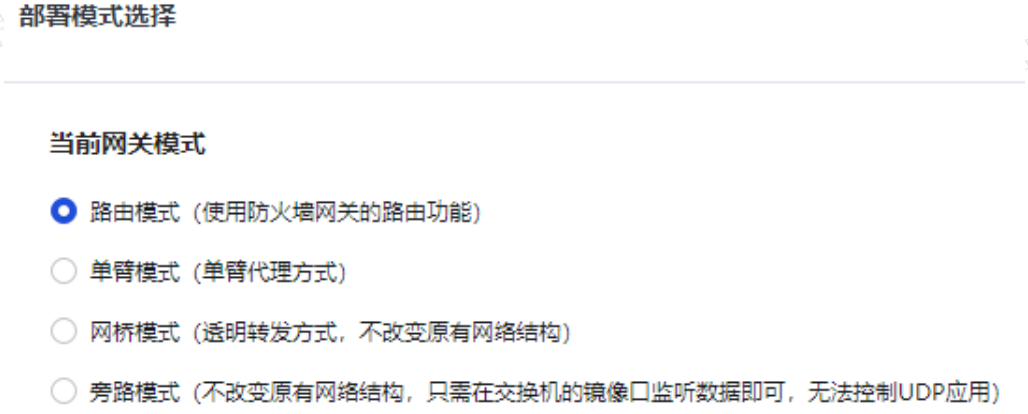
路由模式：当需要设备参与路由转发时，将设备部署模式修改为路由模式部署，该模式支持AC所有功能。

网桥模式：可以把设备视为一条带过滤功能的网线使用，通常在不改变原有网络拓扑结构的情况下使用，平滑部署到网络中，可以实现设备的大部分功能；

旁路模式：设备连接在内网交换机的镜像口或HUB上，镜像内网用户流量数据，实现对内网数据的监控和控制，无需改变用户的网络架构，并且可以避免设备对用户网络造成中断的风险，但这种模式下设备的控制能力有限制，部分功能无法实现。

单臂模式：设备连接到交换机，作为代理服务器代理内部PC上网，使上网数据经过设备，实现权限控制和审计功能，无需改变用户网络拓扑。

选择导航菜单中的[系统管理/网络配置/部署模式]，进入部署模式编辑页面，点击<开始配置>，出现路由模式、单臂模式、网桥模式、旁路模式的选项，选择需要配置的部署模式。



将设备部署到网络前，建议先完成设备的部署模式、接口、路由、DNS等信息配置。

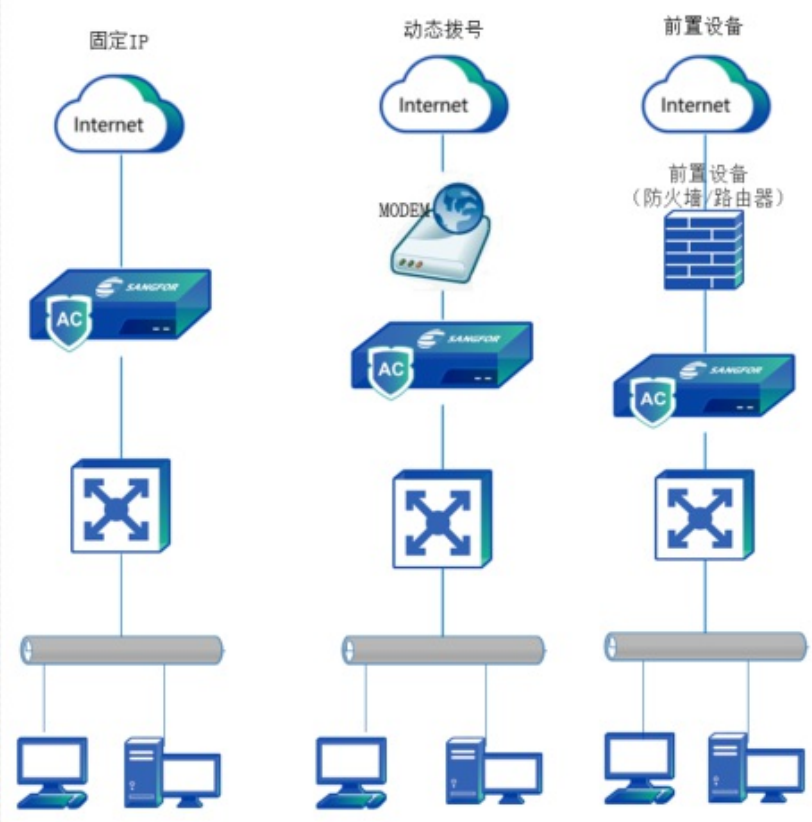
表4设备出厂的默认IP

接口	IP地址
ETH0（LAN）	10.251.251.251/24
ETH1（DMZ）	10.252.252.252/24
ETH2（WAN1）	200.200.65.61/22

路由模式

将全网行为管理AC作为一个网关设备，通常把设备部署在互联网出口位置，代理局域网上网；或者把设备部署在出口网关后面。

部署场景



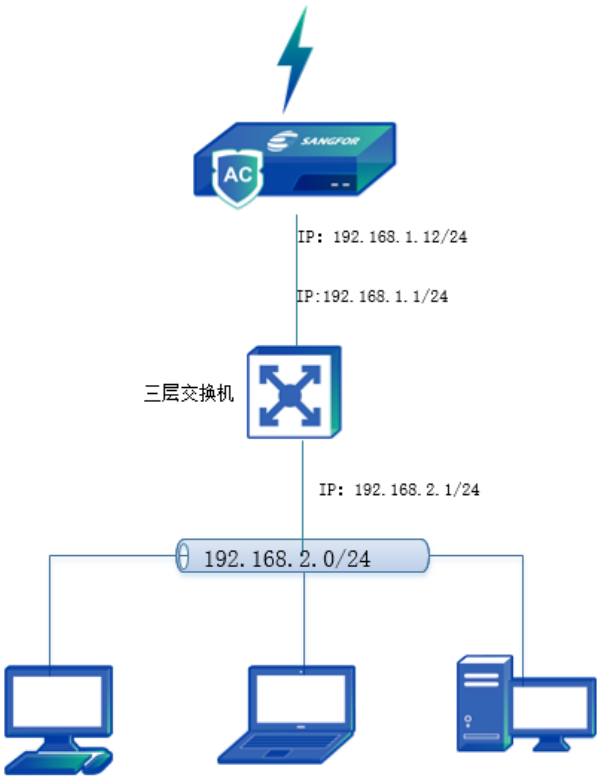
注意事项

1. 设备工作在路由模式时，局域网内电脑的网关指向设备的LAN口IP或指向三层交换机，三层交换机默认路由指向设备。上网数据由设备NAT或路由转发到互联网。
2. WAN、LAN、DMZ网口应设置不同网段的IP地址。
3. LAN口配置802.1Q－VLAN地址后，LAN口可以接支持VLAN的2层交换机的TRUNK口，设备可以在VLAN间转发数据（单臂路由），并可做LAN<->LAN方向的防火墙规则，即可以控制不同VLAN ID之间的访问控制。
4. 如果设置路由模式为ADSL拨号上网，请在配置WAN口IP时选择PPPOE拨号，然后填入拨号账号以及密码。
5. 如果AC设备前有网关设备，请在配置WAN口IP为与前置网关设备LAN口同网段IP；如NAT在前置网关设备配置，AC设备部署完成后，需要在[系统管理/防火墙/NAT代理上网]禁用部署模式生成的NAT策略。

6. 如果前置设备设置了DHCP，WAN口可以设置成自动获取IP，并确保WAN口和DHCP服务器的正常通信。

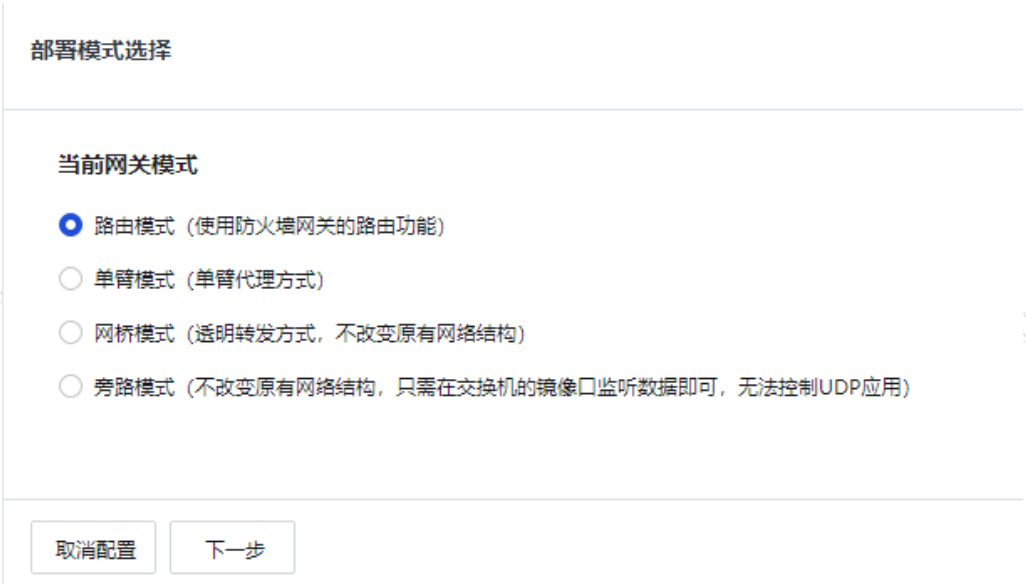
配置指导

用户网络是跨三层的环境，购买设备作为互联网出口网关使用，代理内网用户上网，公网线路是光纤接入固定分配IP。

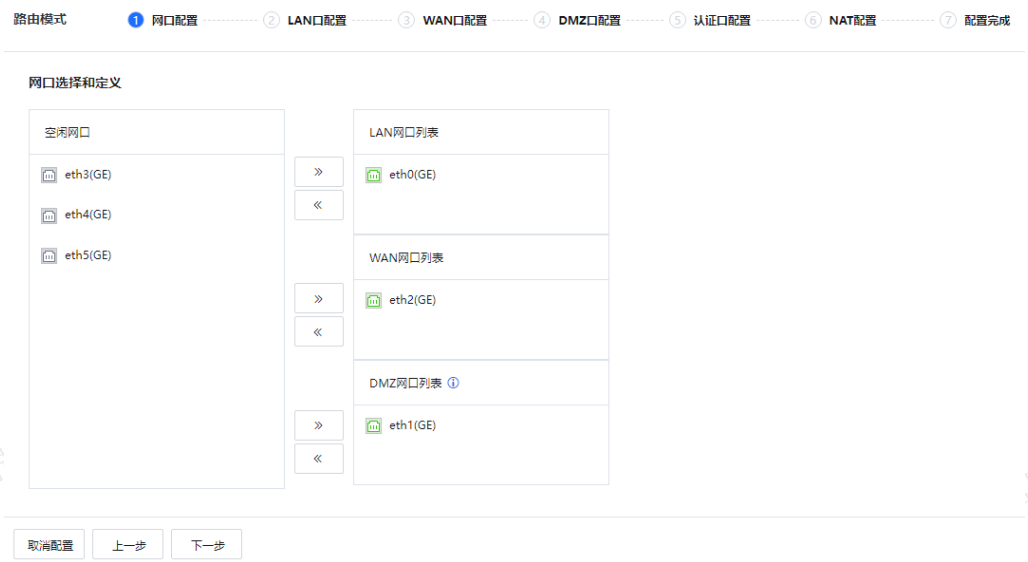


步骤1.通过默认IP登录设备，比如通过LAN口登录设备，LAN口的默认IP是10.251.251.251/24，在电脑上配置一个此网段的IP地址，通过https://10.251.251.251登录设备，默认登录用户名/密码是：admin/admin。

步骤2.在导航菜单页面中的[系统管理/网络配置/部署模式]，右边进入[部署模式]编辑页面，点击<开始配置>，配置设备部署模式为路由模式，点击<下一步>。



步骤3.定义LAN网口和WAN网口，选择空闲网口，点击<增加>，将空闲网口移动到对应的网口列表（设备默认的LAN为ETH0，DMZ为eth1，WAN为ETH2，默认网口位置建议不调整，和设备面板的图示接口保持一致，其他空闲接口可以自定义其所属的区域）。



• LAN网口列表：添加到LAN网口列表中的网口，作为内网口使用，即需要将LAN区网口接到内网方向。

• WAN网口列表：添加到WAN网口列表中的网口，作为外网口使用，即需要将WAN区网口接到外网方向。当需要使用多个WAN口时，需要申请多线路授权。

• DMZ网口列表：添加到DMZ网口列表中的网口，作为内网口使用。通常在DMZ区接入对外发布的内网服务器，同时也可通过设备的防火墙设置控制LAN口区内网用户的访问权限，保证服务器的安全。参考防火墙设置。

步骤4.完成网口定义，点击<下一步>，配置LAN区网口IP地址。此例中LAN口区的网口是ETH0，此处配置ETH0的地址是：192.168.1.12/255.255.255.0。

• 全网行为管理AC版本支持IPV6版本，设备网口IP地址、网关、DNS等均支持配置IPV6地址，以下配置以IPV4配置为例。

• 如果交换机上划分了VLAN，且接设备LAN口为trunk口则需要启用VLAN（本例中接的是三层交换机，不需要启用VLAN）。

• 在IP地址中分别填写各个VLAN的ID及IP，此IP是分配给设备的一个VLAN的空闲IP，如局域网中有VLAN 2，且VLAN 2的网段为10.10.0.0/255.255.0.0，假设10.10.0.1这个IP在内网没有被使用，则可以在IP地址列表中填写10.10.0.1/255.255.0.0。其他的VLAN信息也按照这种方法，一行一个添加进去。

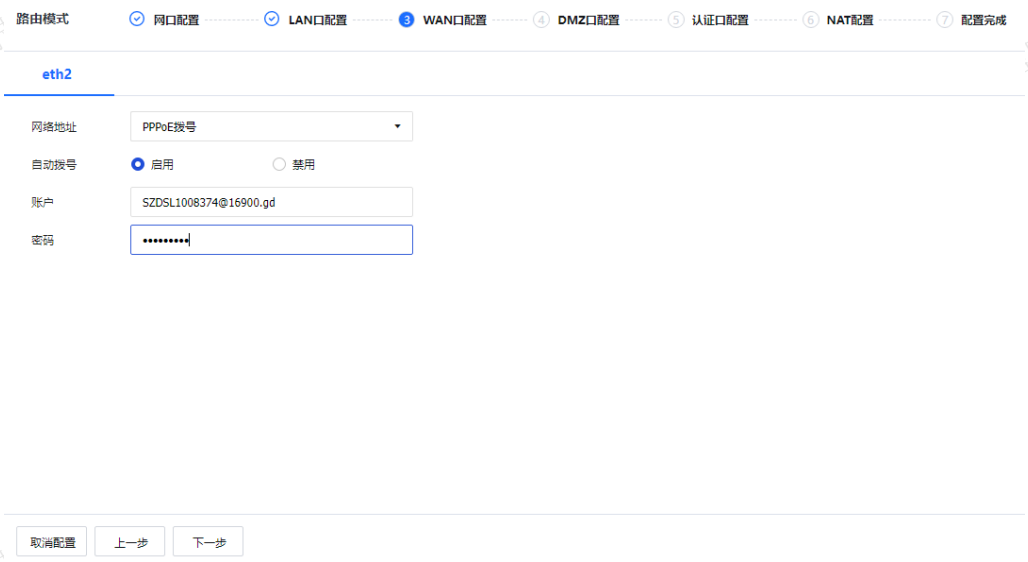
步骤5.配置WAN区网口，此例中WAN口区的网口是ETH2。

• 配置WAN区网口，此例中WAN口区的网口是ETH2。

• WAN口支持自动获取、手动配置和PPPOE拨号三种类型，此例中公网线路是光纤接入，固定分配公网IP地址的，所以选择[手动配置]。

• 如果公网IP是通过DHCP自动获取的，那么请勾选自动获取，此例中公网IP已经固定分配了，在[IP地址]中填入公网IP地址，另外分别配置好公网分配的网关地址、DNS。

步骤6.如果线路是PPPOE拨号，需要将WAN口和modem相连。勾选自动拨号作用是在拨号线路异常断开后自动重新拨号，或者是重启设备后自动拨号。输入拨号的账号和密码。

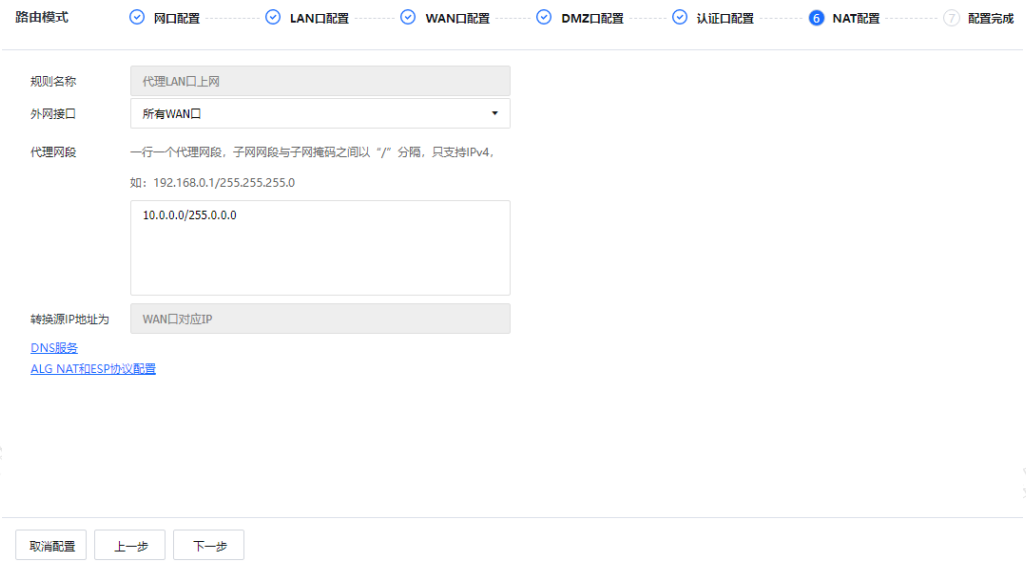


步骤7.配置DMZ区网口，此例中DMZ区网口是ETH1，在IP地址栏配置IP地址和子网掩码。

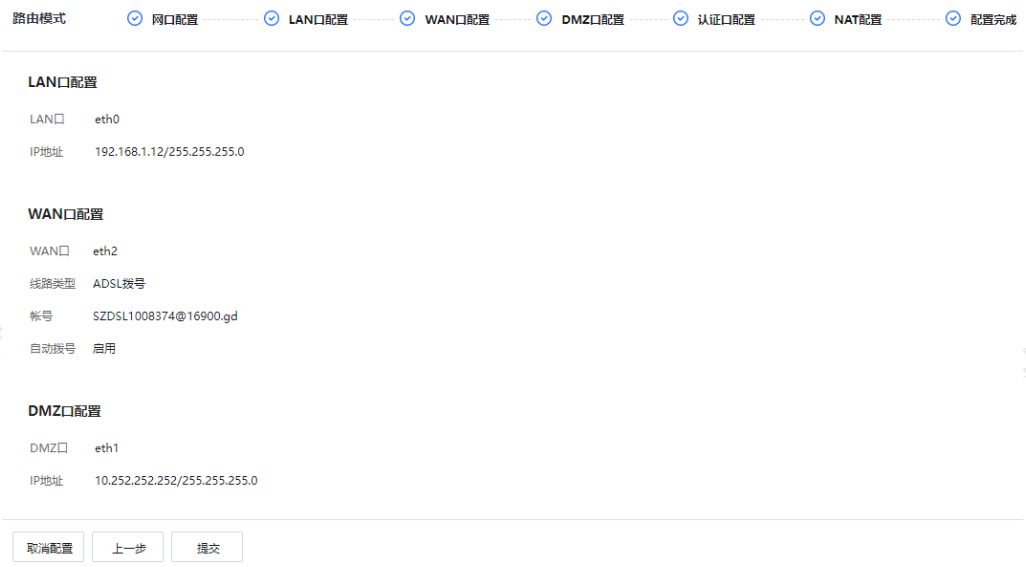
步骤8.AC设备使用认证中心相关功能时需要配置认证口，给分支AC做认证托管功能使用，常规的旁路部署、网桥部署、路由部署无需设置认证口。

步骤9.NAT配置，用于设置代理上网规则，当设备做网关，接到公网线路时，需要在设备上做代理上网设置，以代理内网用户正常上网。设置要代理的[代理网段]并指定[外网接口]，[外网接口]可以设置为WAN区的其中一个网口或者全部网口。

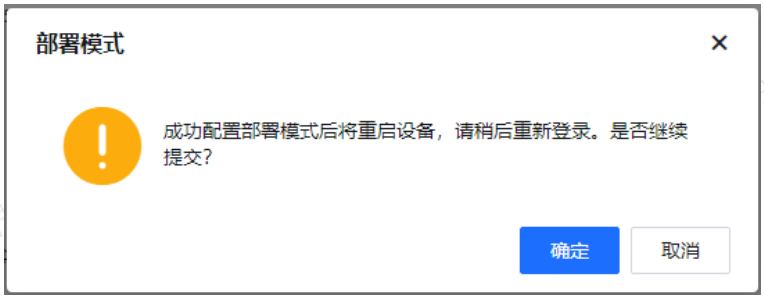
完成部署模式向导后，在[系统管理/防火墙/NAT代理上网]中会新增一条代理规则“代理LAN口上网”，此处不能修改名称和转换的源地址，如果需要配置请在[NAT代理上网]中进行配置。如果内网还有其他网段的用户需要被代理，也需要在[NAT代理上网]中另外添加规则参考NAT代理上网。



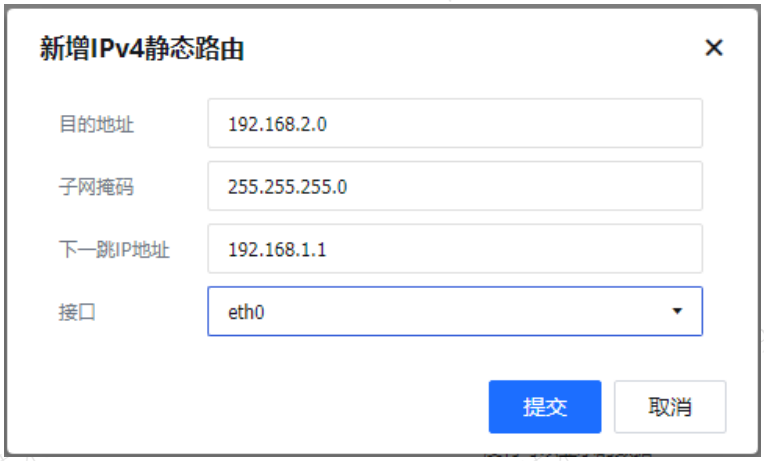
步骤10.检查配置无误后，点击<提交>。



步骤11.设置完毕需要重启设备才可以生效，在弹出的提示框中点击<是>。



步骤12.此例中由于内网的网段与设备LAN口不在同一网段，需要在设备上添加到内网的路由条目，在导航菜单页面中的[网络配置/静态路由]，右边进入静态路由编辑页面，点击<新增>则可以添加路由（具体设置方法参考路由章节）。当内网有多个网段时需要相应的添加多条静态路由。



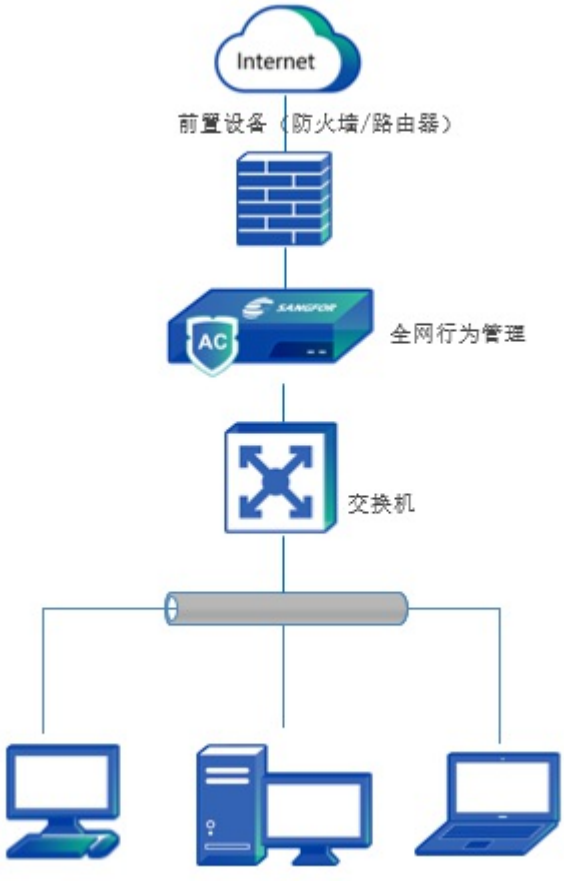
步骤13.基本配置完毕后，将设备接入网络中，WAN口接外网线路，LAN口接内网交换机，并且将内网交换机的路由重新指向设备的LAN口。

网桥模式

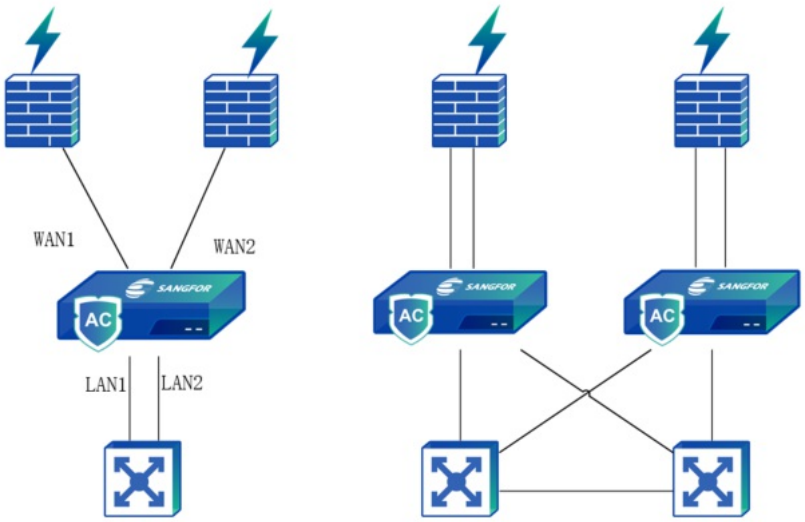
网桥模式是把设备视为一条带过滤功能的网线使用，通常在不改变原有网络拓扑结构的情况下启用。把设备部署在原有网关与内网用户之间，在原网关和内网用户不需做任何配置改变的情况下，即可实现设备功能。网桥模式的主要特点是对用户做到完全透明。

部署场景

• 场景一：设备单网桥部署。适用于网络一进一出场景。



• 场景二：设备多网桥部署。适用于用户内网存在VRRP或HSRP，或网络中存在双机高可用场景。设备多网桥部署实现访问控制、审计功能的同时，不影响用户原有主备的切换。如图所示的两种运行环境。

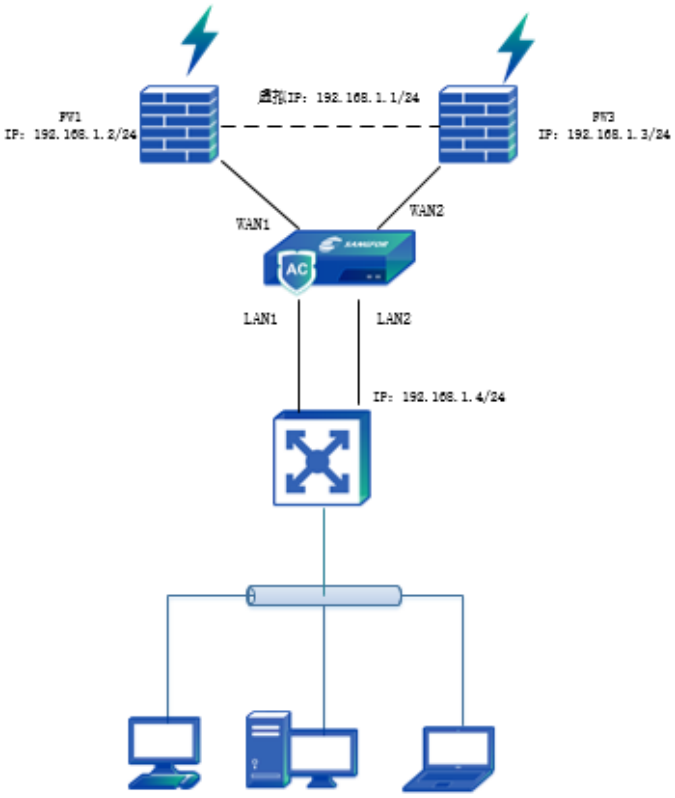


注意事项

1. 设备工作在网桥模式时，内网电脑的网关不需要改变，保留指向原有网关即可（即指向前置设备的内网接口IP）。
2. 设备工作在网桥模式时，需要注意接口方向，保证WAN区接前置的路由设备，LAN区接内网的交换机。数据从LAN区发送到WAN区才可以进行用户认证、上网权限控制和审计。
3. 设备的网桥模式是在数据链路层（OSI第二层）上实现的透明，是通过把设备的网口桥接起来实现的。数据链路层及以上各层的数据均可穿透。原有网关启用IP/MAC绑定及DHCP等需要第二层数据穿透的功能可以正常使用。
4. 在网桥模式下设备无NAT功能，VPN功能不生效。
5. 如启用上网安全、邮件内容识别等功能或要让设备能够自动升级URL库，应用识别规则库，杀毒引擎等，则需配置网桥IP，默认网关和DNS，并保证设备本身访问外网（可通过升级控制台工具ping测试）。
6. 如启用WEB认证、准入客户端推送或其他需要重定向到设备上的功能，同时内网有多网段时，须添加到内网非直连网段的路由指向内网路由设备。
7. 网桥模式时，设备网桥支持VLAN TRUNK穿透，网桥的IP地址支持802.1Q-VLAN的地址，即设备可以透明接在VLAN TRUNK的主干道上。

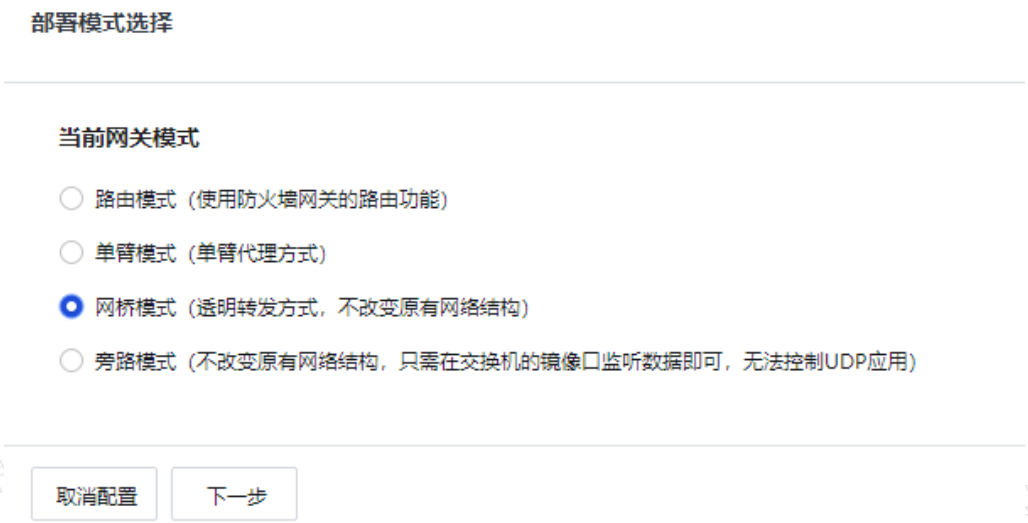
配置指导

以设备多网桥部署为例，用户的两台FW内网接口运行VRRP协议，FW对应的虚拟IP是192.168.1.1，交换机上联两台FW的接口处于同一个VLAN，VLAN接口IP为192.168.1.4，设备双进双出做双网桥部署在交换机和防火墙之间。

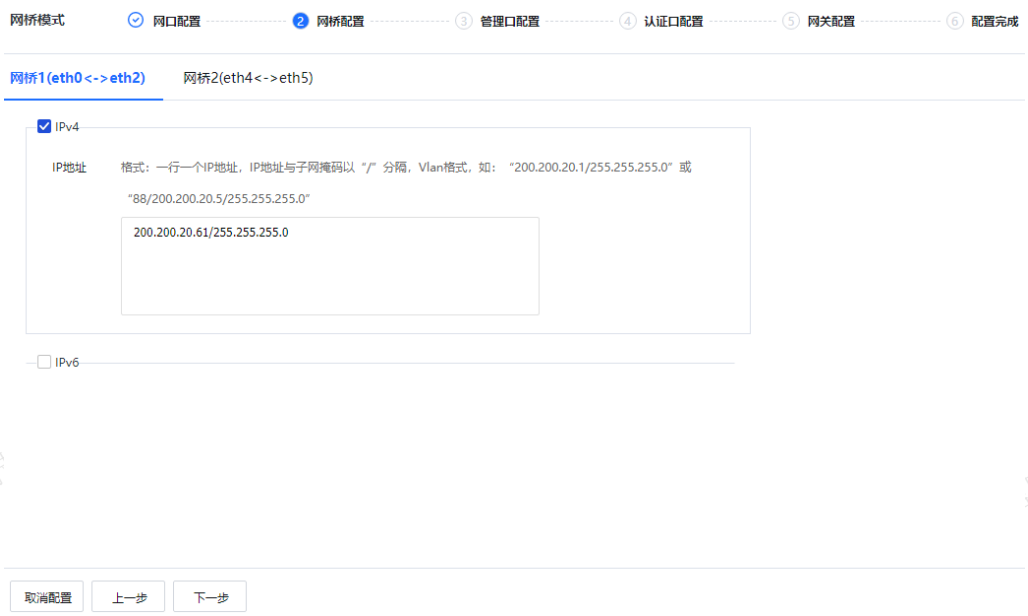


步骤1.通过默认IP登录设备，比如通过LAN口登录设备，LAN口的默认IP是10.251.251.251/24，在电脑上配置一个此网段的IP地址，通过https://10.251.251.251登录设备，默认登录用户名/密码是：admin/admin。

步骤2.在导航菜单页面中的[系统管理/网络配置/部署模式]，进入[部署模式]编辑页面，点击<开始配置>，配置设备模式为网桥模式，点击<下一步>。



步骤3.分别选择LAN区网口和WAN区网口，组成两对网桥，如图所示。



• [LAN网口选择]用于选择内网接口。

• [WAN网口选择]用于选择外网接口。

• [网桥列表]用于定义网桥，每对网桥接口之间允许转发数据，非网桥对接口之间的数据不允许转发。

• [开启多网桥链路同步]当网桥的一个网口由连接到断开或者是从断开到连接，另外一个网口的状态完成相应的转换，实现同一个网桥的两个网口状态同步，通常用于在冗余网络环境中通知对端设备该链路正发生了故障或已从故障中恢复，建议开启。

步骤4.网桥配置，配置网桥IP地址。

• 在[网桥配置]中配置设备网桥1的IP地址，此例中由于两个网桥处在相同网段，只能配置一个IP地址。（如果网桥处于不同的网段，可以按照网络中空闲的IP地址分配两个网桥用做网桥IP）

• 如有VLAN数据穿过设备，并且网桥IP属于某个VLAN，配置网桥IP时需要加上VLAN标签信息（常见场景：1、AC设备桥接在2台交换机之间，并且交换机互联接口均为trunk模式；2、AC上连路由器，下联交换机，路由器配置单臂路由，交换机接口配置trunk模式）。

• 此处如果没有多余的空闲地址分配做网桥IP，不会影响内网用户访问互联网，但此时设备没有有效的IP地址和内网、外网进行通讯，某些功能会受到影响，比如：规则库更新、WEB认证、准入客户端推送等，这

种情况可以通过管理网口接到内网交换机上，通过管理网口实现设备和内外网的通信。

• 网桥部署模式下网桥IP可以为空。

• 多网桥下各组网桥之间的IP不能同网段，而且网桥之间不能有相同的VLAN ID。

步骤5.配置管理网口DMZ接口，选择一个设备空闲的网口（非网桥口）作为管理网口。

步骤6.AC设备使用认证中心相关功能时需要配置认证口，给分支AC做认证托管功能使用，常规的旁路部署、网桥部署、路由部署、单臂模式无需设置认证口。

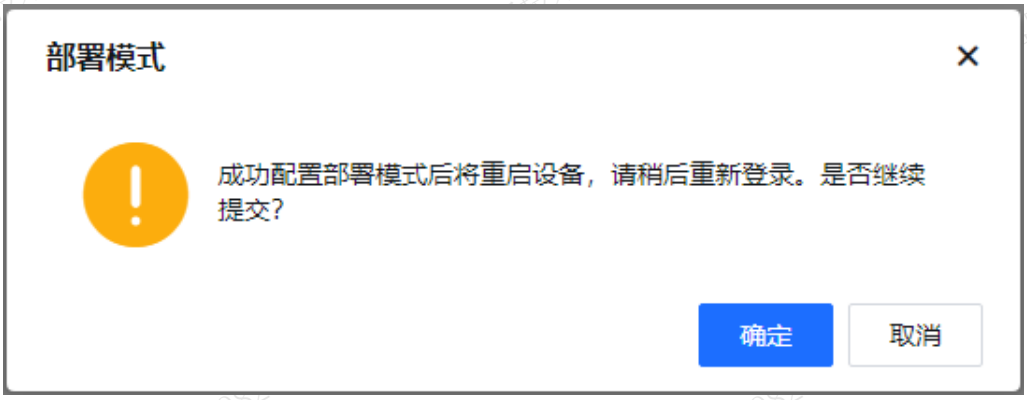
步骤7.网关配置，配置网关地址，DNS地址。

• 在[网关配置]中配置设备默认网关和DNS地址。此例中默认网关指向前置FW的虚拟IP地址，DNS设置网络运营商分配的公网DNS地址。

• 勾选[自动放通防火墙规则]：用于放通WAN<->LAN方向所有数据的防火墙规则。

步骤8.确认配置信息，确认无误后，点击<提交>。

步骤9.设置完毕需要重启设备才能生效，在弹出的提示框中点击<是>。



步骤10.基本配置完毕后，将设备接入网络中，WAN1口、WAN2口分别接FW1、FW2，LAN1口、LAN2口

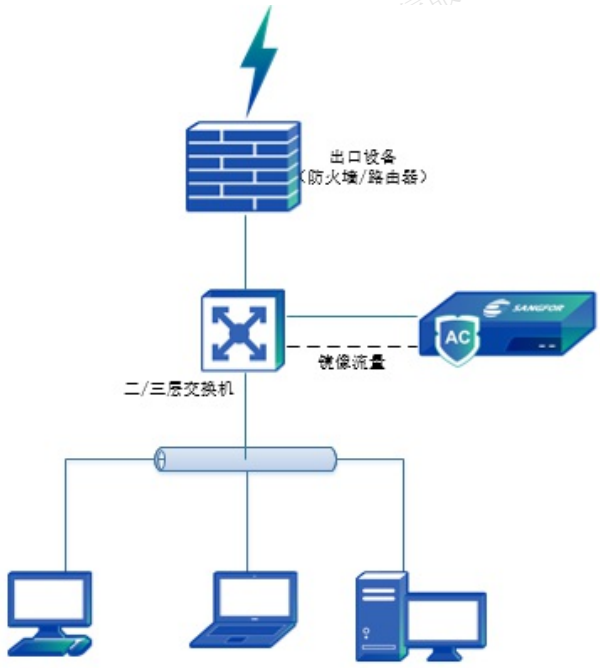
接内网交换机。

旁路模式

旁路模式不需改变用户的网络环境，并且可以避免设备对用户网络造成中断的风险。用于把设备接在交换机的镜像口或者接在HUB上，保证内网用户上网的数据经过此交换机或者HUB，并且设置镜像口的时候需要同时镜像上下行的数据，从而实现对上网数据的监控与控制。

如果旁路部署的全网AC开启了802.1x准入功能，当AC宕机时会造成入网用户无法通过认证导致断网的情况。如果在交换机上开启了802.1X逃生功能，旁路部署的AC宕机后入网用户无需认证直接入网，不会对入网用户造成断网影响。

部署场景

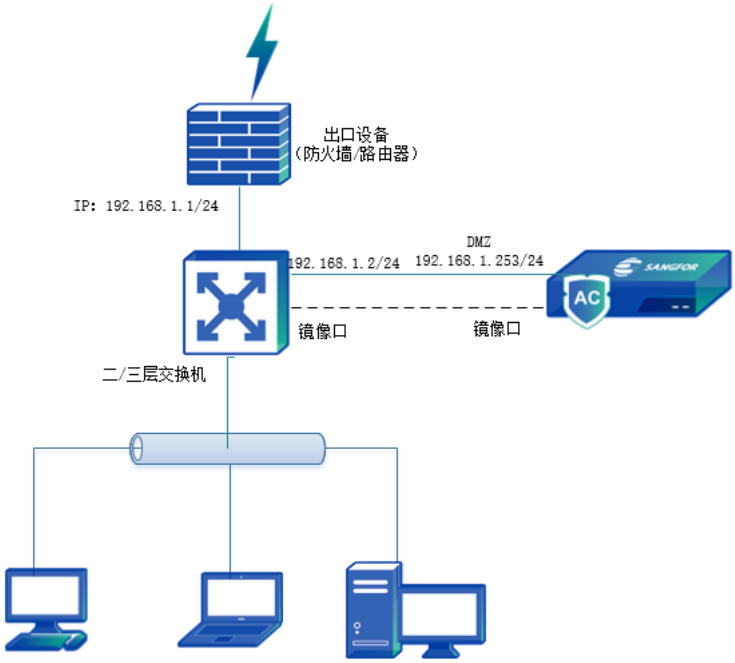


注意事项

1. 用户必须使用HUB或者交换机具有镜像口的情况。如果交换机没有镜像口，可以在交换机前加接HUB实现。
2. 旁路模式下，流量显示、活动连接排名显示无效。
3. 旁路模式下，TCP的控制是通过DMZ口发送reset包实现的，因此要保证DMZ口发送的reset包都能被PC和公网服务器收到。
4. 旁路模式下很多功能不能实现，比如VPN、DHCP等。
5. 旁路模式主要起监控的作用，限制的功能没有路由模式和网桥模式那么全面。只能对TCP的连接进行限制，比如URL过滤，关键字过滤，邮件过滤等。对UDP不做限制，比如P2P软件，QQ的登录等。
6. 旁路模式下，只有在WAN口接镜像口的情况下，网关运行状态才会显示流量图，且在接了WAN口的情况下，网络接口状态下只有接收流量没有发送流量。

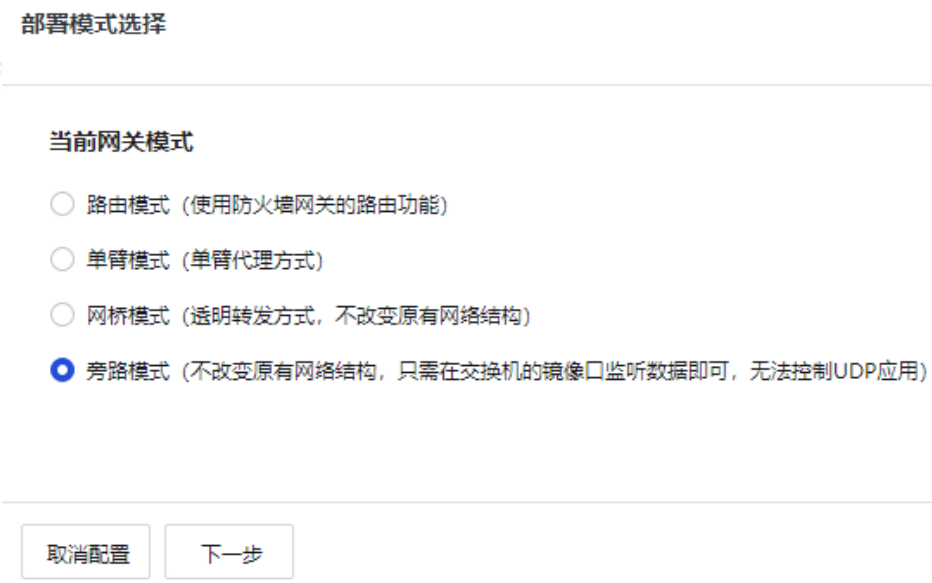
配置指导

拓扑如下图所示，设备做旁路模式，交换机通过镜像口把流量镜像到AC设备镜像口，监控内网各个网段的上网数据，内网用户使用WEB认证。AC设备DMZ管理口连接交换机，并且分配一个可使用的业务IP地址，设备通过此地址完成和公网、内网的通信，设备可以自动更新内置规则库，管理员可以在内网登录设备控制台进行管理。



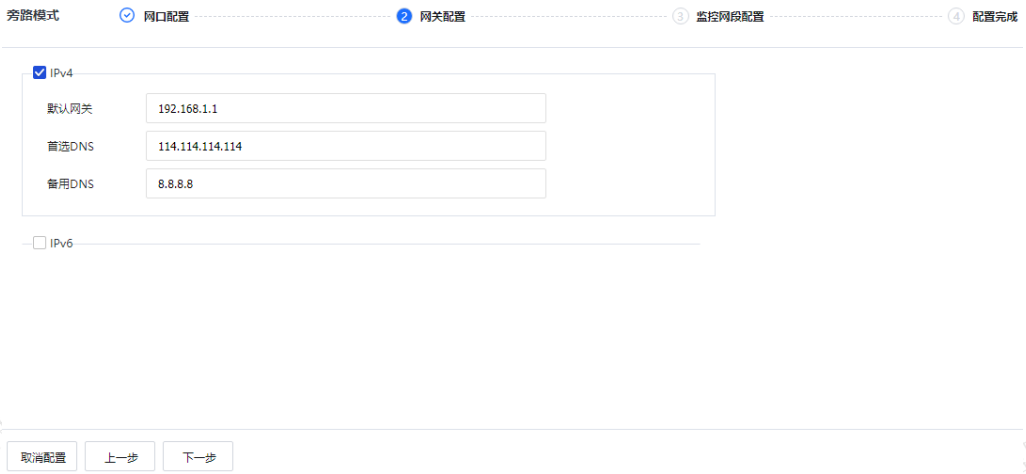
步骤1.通过默认IP登录设备，如通过LAN口登录设备，LAN口的默认IP是10.251.251.251/24，在电脑上配置一个此网段的IP地址，通过https://10.251.251.251登录设备，默认登录用户名/密码是：admin/admin。

步骤2.在导航菜单页面中的[系统管理/网络配置/部署模式]，右边进入部署模式编辑页面，点击开始配置，出现以下页面，配置设备模式为旁路模式，点击<下一步>。



步骤3.配置管理网口地址：旁路模式下，管理网口默认选择ETH0口，可选择修改。认证口按需配置，一般是在分支AC需要做认证托管时，将认证口发布到公网的情况，认证口为了安全部分端口不放开为WAN属性，如果是内网使用，建议只启用管理口。

步骤4.配置管理口DMZ网关、DNS，实现内外网通信。



- [IP地址]填写分配给设备管理口(DMZ接口)的IP地址，此例中需要将DMZ口接到内网交换机上，所以填写一个可以和交换机以及内网通信的IP地址。
- [默认网关]指的是设备的网关，此例中填写和DMZ口连接的交换机的网口地址。
- 在[首选DNS]和[备用DNS]中填写公网可以使用的DNS地址。

步骤5.选择设备镜像口，配置需要监控的内网网段和服务器列表。

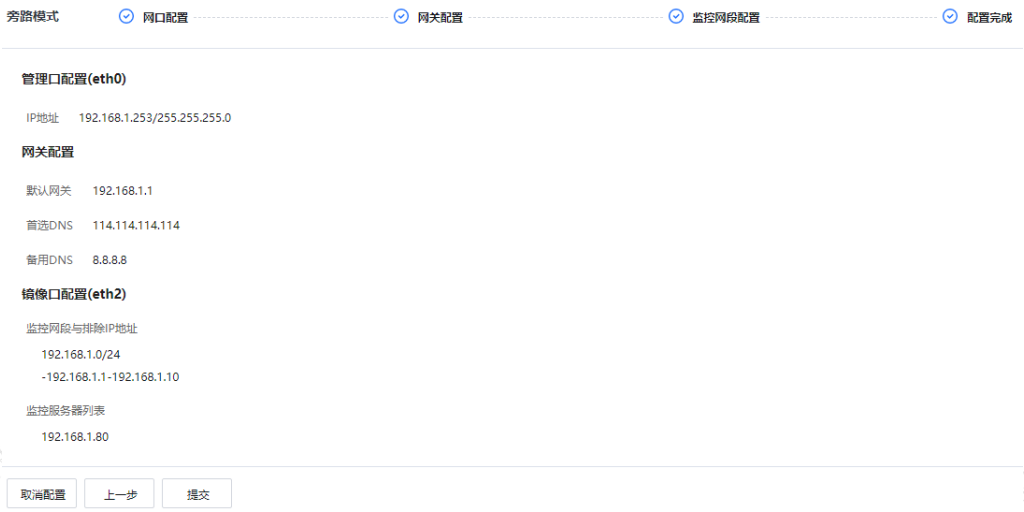
• 选择镜像口，配置监控网段和监控服务器列表。

• [监控网段与排除IP地址列表]：中填写需要监控的网段，以及需要排除监控的地址。此处填写内网的网段192.168.1.0/255.255.255.0，则此时这个网段访问其他网段的数据都会被监控，这个网段之间的访问不会被监控。排除网段用192.168.1.1-192.168.1.10表示，填入后表示192.168.1.1-192.168.1.10这个范围内的IP访问其他网段（外网）的数据不会被监控。

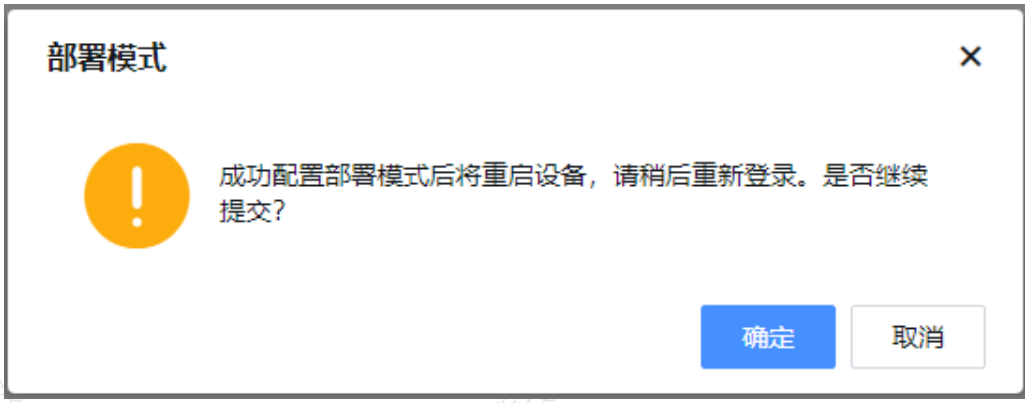
• 高级配置中用于设置[监控服务器列表]，填入列表中的地址，在被监控网段中的IP访问时，数据也会被监控。例如内网有一台web服务器，用户想要记录内网用户访问这台服务器的数据，因为同一网段的访问是不会被监控的，此时，将web服务器的IP地址填写到[监控服务器列表]中即可。

• 以上说的是监控的设置，因为旁路模式下可以实现部分TCP控制功能，控制功能是在监控的基础上实现的，也就是说能监控的数据才能被控制。

步骤6.确认配置信息，点击<提交>。



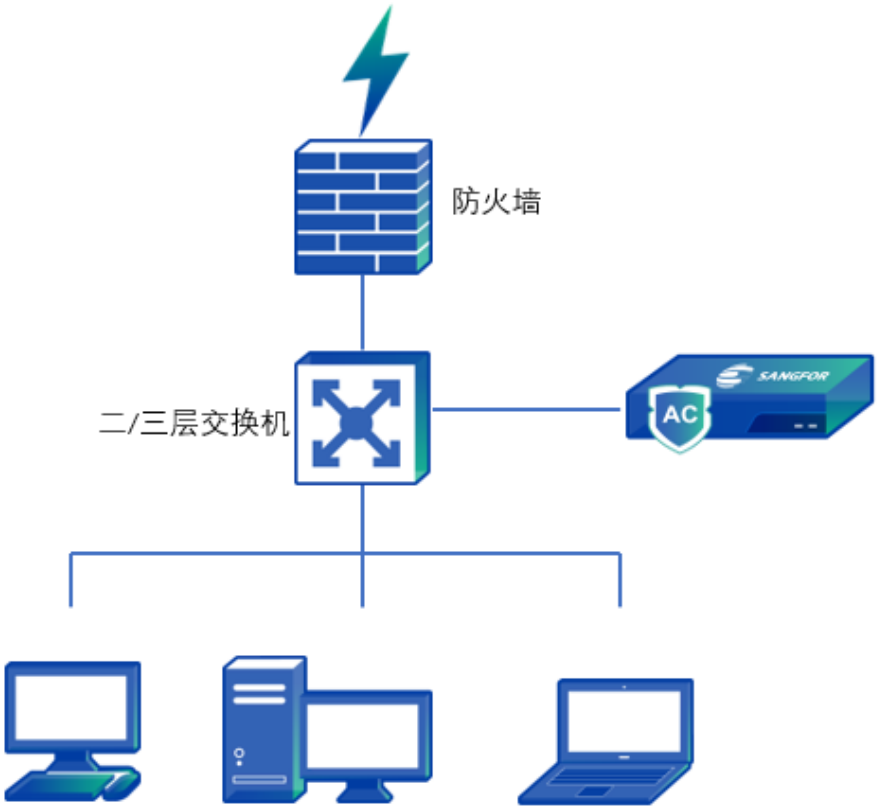
步骤7.设置完毕需要重启设备才可以生效，在弹出的提示框中点击<是>。



单臂模式

单臂模式是在全网行为管理AC开启代理模块，作为代理服务器代理内部终端上网，使上网数据经过设备，实现控制和审计功能。AC设备连接到交换机，部署无需改变用户网络拓扑，对用户的网络环境不会造成影响。

部署场景

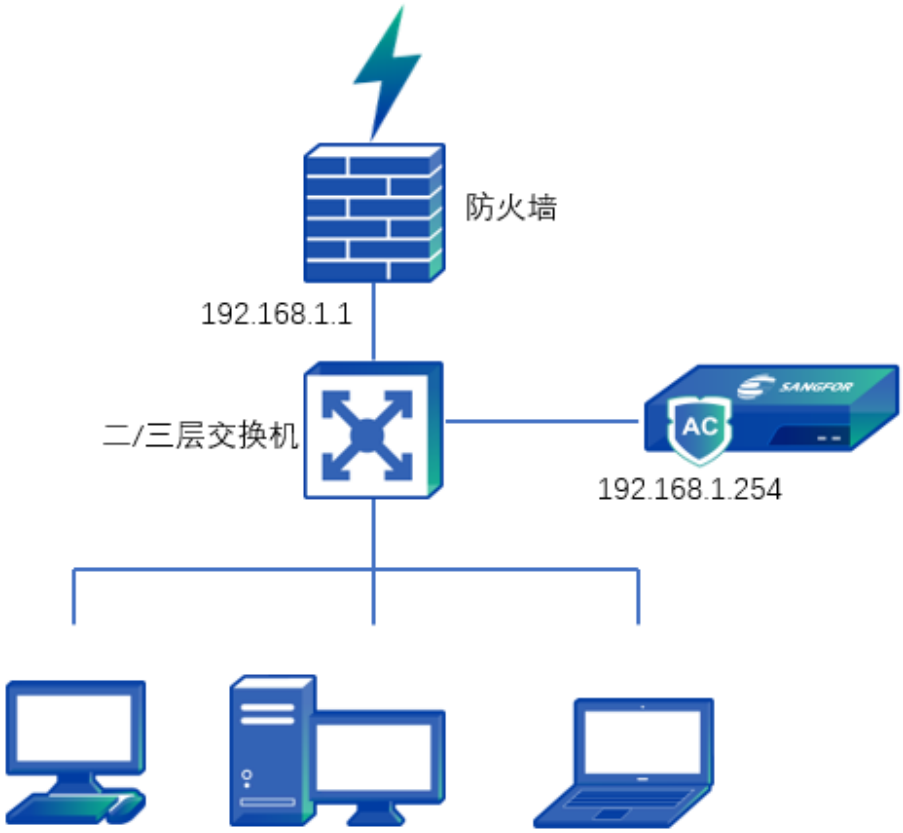


注意事项

1. 开启HTTP代理，认证策略如果设置密码认证，默认终端弹出的密码认证页面是微软的认证页面，如果客户需要弹出AC的Web认证页面，需要在[接入管理/接入认证/认证高级选项]勾选“代理上网时，密码认证使用WEB认证页面”，但是该功能只对http显示代理有效。
2. 启用代理服务，如不配置代理策略，默认允许内网所有用户通过代理上网。
3. 配置多条代理策略时，策略匹配顺序为从上往下匹配。
4. 确保设备本身可以正常访问互联网，并且内网PC和设备之间通信正常。

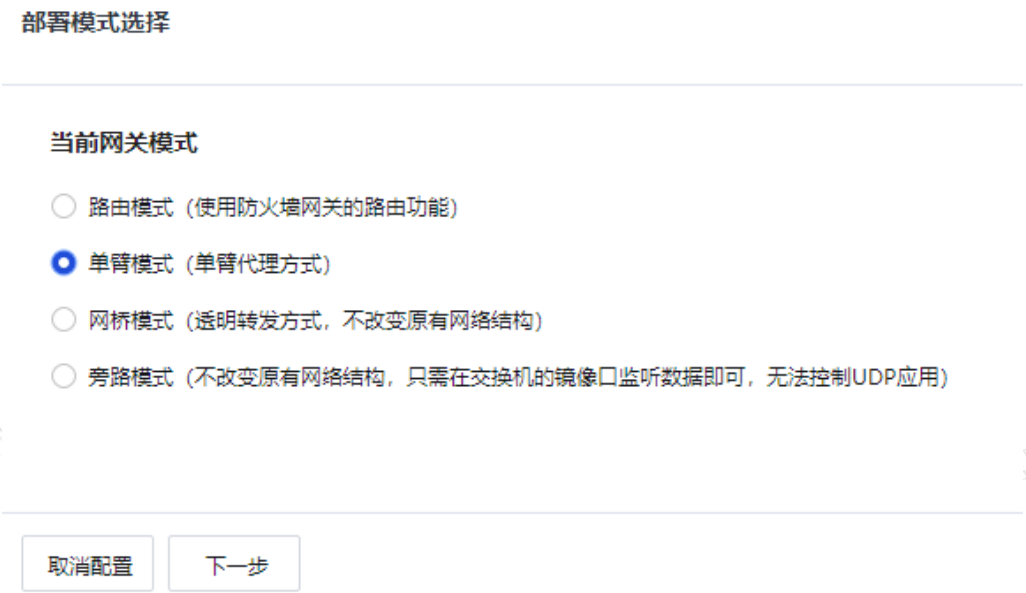
配置指导

如下图所示，设备部署为单臂模式，启用上网代理功能。受防火墙安全策略管控，终端用户无法直接访问互联网，网络中只允许AC设备访问互联网，终端用户可以和AC设备正常通信。AC设备作为代理服务器代理内部终端上网，使上网数据经过设备，实现访问控制和审计功能，无需改变用户网络拓扑。



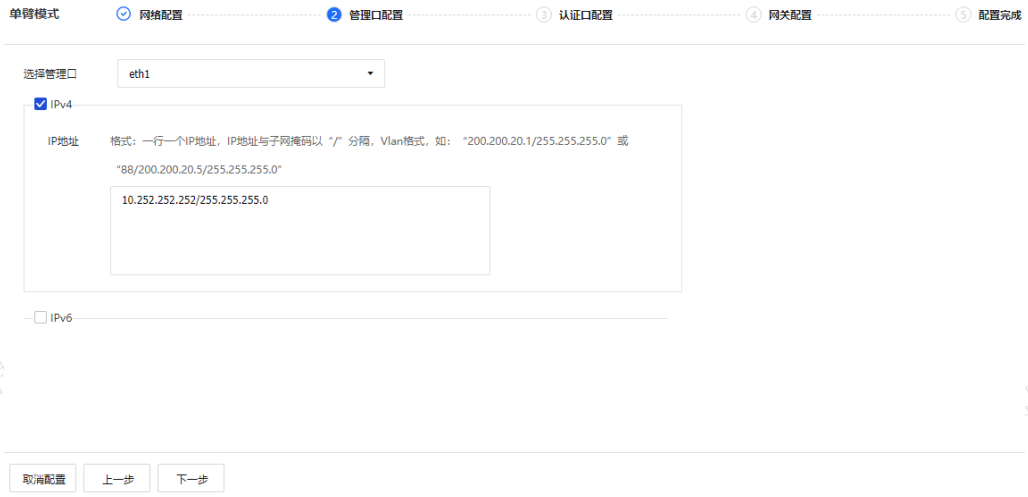
步骤1.通过默认IP登录设备，比如通过LAN口登录设备，LAN口的默认IP是10.251.251.251/24，在电脑上配置一个此网段的IP地址，通过https://10.251.251.251登录设备，默认登录用户名/密码是：admin/admin。

步骤2.在导航菜单中的[系统管理/网络配置/部署模式]，右边进入部署模式编辑页面，点击<开始配置>，配置设备模式为单臂模式，点击<下一步>。



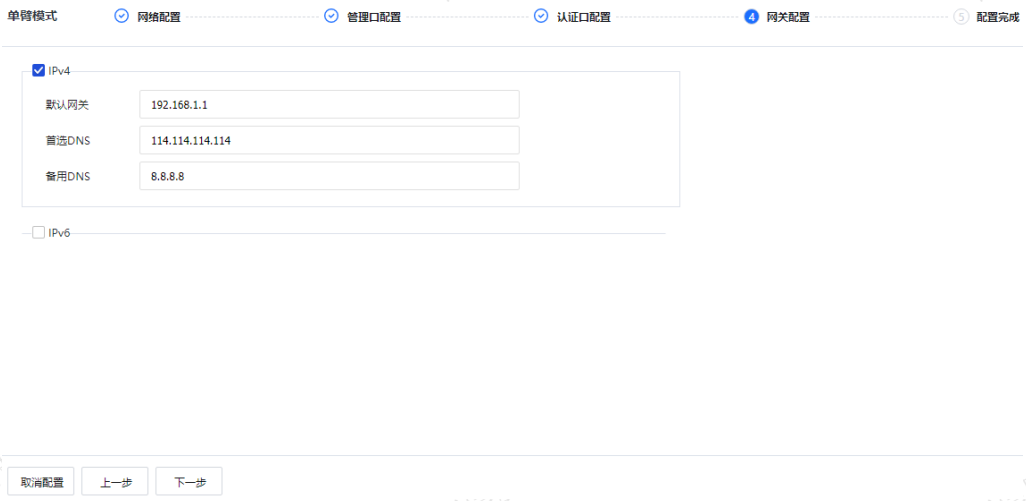
步骤3.选择eth0口，需要将设备的eth0口接到交换机上，并配置接口IP，支持配置IPV6地址，配置完成后，点击<下一步>。

步骤4.管理口配置：选择空闲的网口做为管理网口，用户可以通过此网口连接设备，默认情况下设备的管理网口是eth1口；支持配置IPV6地址，配置完成后，点击<下一步>。



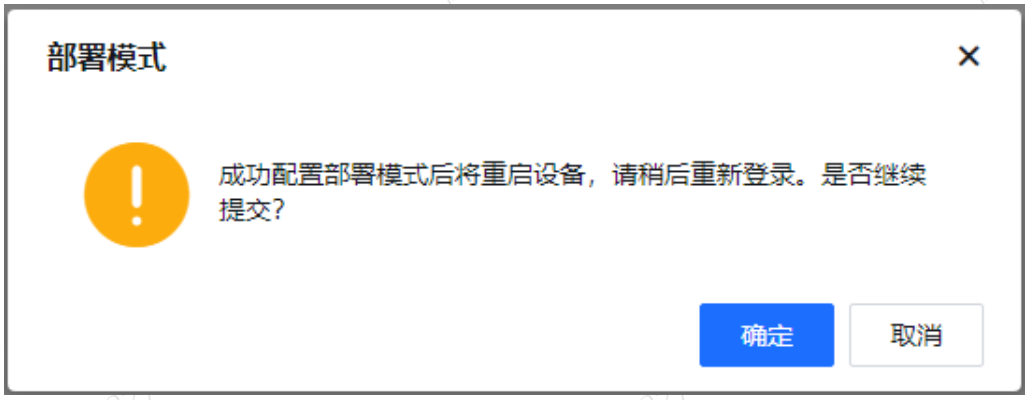
步骤5.AC设备使用认证中心相关功能时需要配置认证口，给分支AC做认证托管功能使用，常规的旁路部署、网桥部署、路由部署、单臂模式无需设置认证口。

步骤6.配置AC设备网关（eth0接口，非管理口网关）以及DNS等信息，配置完成后，点击<下一步>。



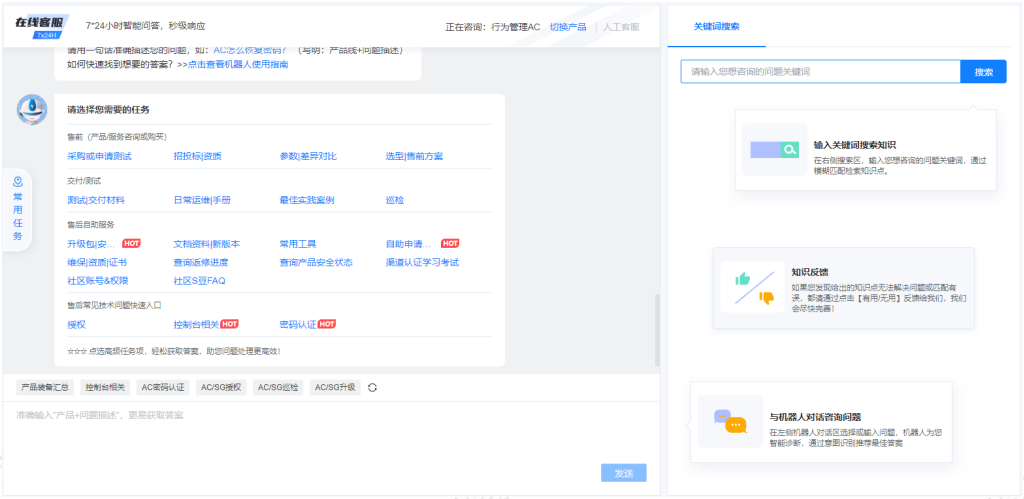
步骤7.配置完成，检查各配置项信息，点击<提交>。

步骤8.设置完毕需要重启设备才可以生效，在弹出的提示框中点击<是>。



在线客服

设备的控制台合入社区机器人，日常咨询小问题都可以找机器人，一秒解决您的问题。当设备可以联网的时候，在设备的右下角点击机器人的头像 就可以跳转的问题聊天界面。



当设备未联网的时候，会跳转到信服君的二维码界面，可扫描二维码进行咨询。

首页

首页的功能主要是查看当前设备的一些接入状态以及设备的使用状况，能够及时反应全网当前上网的状态信息，主要包括信息概览、流量分析、行为风险分析、系统状态。

信息概览

信息概览主要显示当前的设备状态和管理状态，管理状态中的行为风险分析中的展示模块还可以选择模块进行展示。从而对用户、流量、行为做到可视可控。

设备状

设备状态主要是显示设备的整体使用概况包括：CPU、内存、存储、授权状态。

终端接入安全：当鼠标停留在“接入终端安全”的图标时，可显示终端安全检查、非法外联、外设管控等序列号状态是否有效，点击图标会跳转到授权管理页面。

规则库升级：当鼠标停留在“规则库升级”的图标时，可以查看到URL库、应用识别、审计规则库可以看到相关规则库的版本和升级服务有效期。

软件升级：当鼠标停留在软件升级图标时，可显示设备过期的时间，点击“软件升级”图标会跳转到授权管理页面。

管理状态

管理状态主要是显示已接入用户、流量分析、行为日志的整体概况。

已接入用户：可显示当前内网用户上网的总人数、移动终端、共享终端。EDR终端保护点击<未开启>可会跳转到安全能力界面，可设置连接EDR平台，当设备与EDR对接后，内网终端用户可以收到EDR的实时保护，会显示保护状态。

流量分析：设备是以最近1小时内用户使用流量的情况来分析评级。

点击<评级设置>可以设置带宽使用率占比，时长的状况来定义评级的优良情况。管理员可以查看当前最拥堵线路、时长、流量状况，点击<查看详情>可以跳转到系统内置的日志分析平台的带宽分析相关的信息。

行为日志：实时记录内网用户上网的数据，有泄密风险应用、共享接入、怠工人数、违规应用、风险用户的人数。

流量分析

流量分析可以对全局的上网的流量进行分析，包括接口吞吐率折线图-所有WAN口实时流量、用户流量排名、应用流量排名、业务流量排名。

接口吞吐率折线图：设备通过折线图的形式来动态显示外网接口实时发送、接收数据的情况。同时，也能显示一个时间段内接口转发的情况。

用户流量排名：用于显示前八名的用户流量排名情况，可以根据上下行流量、总流速和会话数来排名，用户可设置自动刷新的时间，选择用户名称，显示当前用户的名称显示应用详细的信息。

应用流量排行：用于显示前八名的应用排名情况，可以根据上下行流量和总流速来排名，选中<上行>则显示上行流量的百分比，选中<下行>则显示下行流量的百分比，也可以设置自动刷新时间。

资产分析

资产分析包括资产类型分布、新设备发现趋势、合规检查结果三大模块。

资产分析页面可以查看资产的汇总信息、设备发现趋势以及准入合规的检查结果汇总，直观展示整体资产情况，其中包括PC、移动终端、网络设备、哑终端设备和医疗设备等。

- 资产类型分布通过主动和被动的识别方式获取网络中的各类终端类型，可在首页中设置显示的终端类型。
- 新设备发现趋势用于展示具体到每天发现的终端数，时间段可根据需求设置为最近1天或7天，点击卡片自动跳转到终端列表页面。
- 合规检查结果用于展示网络中不合规的终端数及违规项。

行为风险分析

通过行为风险分析可概览内网用户上网行为，包括泄密风险、终端接入、工作效率、违规访问和上网安全。

行为风险分析的数据是来源于日志分析平台(内置日志中心)的应用分析结果，AC默认关联内置的日志分析平台。

泄密风险：主要是统计内网用户文件外发信息和行为感知APP的泄密风险做联动，来反馈设备当前的用户是否有泄密的风险。

点击 可以设置泄密风险参数设置，包括网络暴露应用、数据外发应用、用户组、数据外发阈值等。

点击<查看详情>可以跳转到内置日志分析平台，可在泄密追溯分析应用进行数据分析。如果应用未安装或未启用，则会提示此APP尚未开启或者是尚未安装。

终端接入：主要用于显示内网用户是否有私接WIFI等操作，会实时显示共享接入的人数。用户点击<查看详情>会跳转到[安全管理/终端防私接/共享接入管理/共享状态列表]，查看更多共享信息。

工作效率：可检测内网用户某个时间段是否有过多使用影响工作效率的应用。

管理员点击右上角的 ，跳转到工作效率参数配置页面，可设置的参数为：工作无关的应用、组织结构、工作时间段等，平均每日工作时长大于60分钟（默认）则视为怠工。点击<查看详情>，会跳转到数据中心应用时长排行，查看更多用户信息。

上网安全：主要展示内网上网安全监控概览，可以看到风险用户情况和具体风险行为次数。点击<查看详情>

，可以跳转到“安全状态”页，查看更多详细信息。

违规访问：可用于查看某个时间段内网用户是否有违规访问。管理员可点击右上角的，可以设置违规访问参数配置，自定义选择访问违规应用、用户组。点击<查看详情>，会跳转到数据中心热门应用排行查看更多用户上网信息。

系统状态

系统状态：主要显示设备当前的系统时间、双机状态、并发会话数的情况。

说明：

当设备是主主模式部署时，双机状态呈现为未启用状态。

全网监控

全网监控可以概览内网全局网络分布使用情况，查看终端设备部署使用情况、IP分配情况、内网中的网络设备（交换机、路由器、防火墙等）的分布使用情况，让管理员能时刻掌握内网IP的使用情况，能更好的进行分配。

入网用户管理

入网用户管理主要是管理已经通过设备认证的在线用户的情况。

可以看到所有通过设备认证的在线用户的登录名（显示名）、所属组、IP地址、MAC地址（默认不显示，如需显示请点击<操作>列表中勾选）、终端类型、认证方式、准入插件安装情况、所属控制器名称（当用户是在分支设备认证上线同时分支设备做了认证托管时可显示分支设备名称）、登录时间/冻结时间、在线时长以及对其进行操作。

在线用户管理

在线用户搜索功能

组织结构：在搜索栏中输入关键字来搜索用户组，查询对应用户组的在线情况。

在线用户管理：可以根据登录名、IP地址、MAC地址来搜索到指定用户。

过滤在线用户

管理员点击<过滤条件>可设置指定的条件查看相应的用户。

用户状态：可以选择所有、已冻结用户、活跃用户。

终端类型：可以选择所有、移动终端、PC、多终端。

准入插件安装情况：可以选择所有、已安装、未安装。

合规检查结果：所有、合规、异常、违规。

过滤对象：启用后可以选择用户过滤、IP过滤、MAC过滤，输入指定的用户名、IP、MAC进行过滤，点击<提交>即可。

冻结在线用

当管理员需要冻结在线用户时，选中一个或多个用户点击<冻结>，可以立即断开选中用户的上网连接，使其不能通过设备上网。

选中用户列表中的用户，点击<冻结>即可选择冻结选中的IP或者用户名，并且设置冻结上网的时间，点击<提交>即可冻结成功。

在用户列表会显示用户冻结的时间和冻结状态和时长。

解冻在线用户

当被冻结的用户需要立即解冻上网时，可以直接选中当前被冻结的用户，点击<解冻>，即可立即解冻该用户。

强制注销在线用户

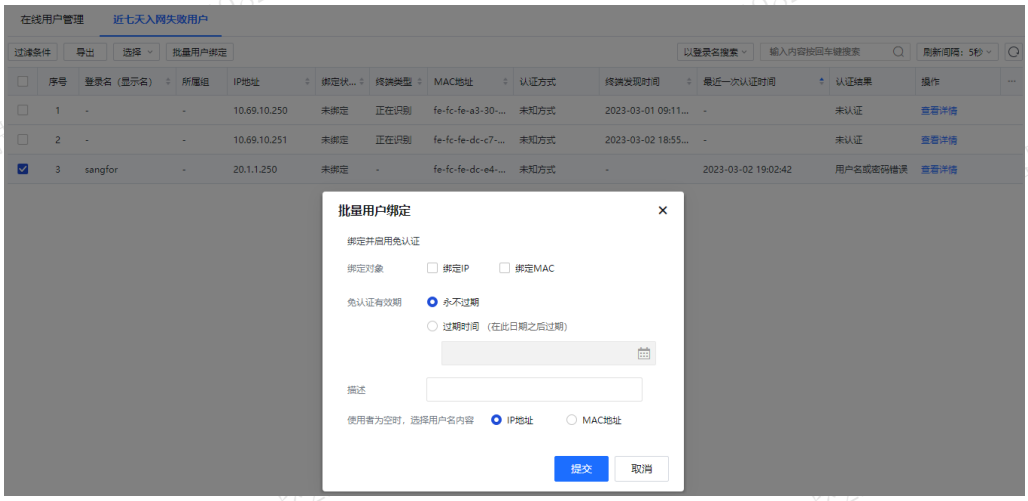
管理员在用户列表中可以强制注销在线用户，但不能对不需要认证、Dkey用户和临时用户进行注销。对密码认证和单点登录的用户可以进行强制注销，注销后用户会下线。

近七天入网失败用户

近七天入网失败用户是用于记录七天内认证失败的用户，支持搜索、过滤、立即刷新、导出等操作。还支持入网识别用户的批量绑定，可对入网失败的用户进行批量勾选并绑定IP/MAC实现免认证上线。

操作步骤

步骤1.当管理员选择识别的用户再点击<批量用户绑定>时跳转到批量用户绑定页面。



步骤2.管理员可选择绑定IP或者绑定MAC来对该用户进行免认证上线。

步骤3.设置免认证有效期：永不过期或者过期时间进行自定义。

步骤4.使用者为空时，选择用户名内容：IP地址或者MAC地址。

步骤5.点击<确定>完成用户免认证绑定。

认证失败的详情可点击<查看详情>跳转到认证失败详情页面，可以看到具体问题描述和修复建议。

全网终端监控

全网终端监控主要用于查看当前内网接入的终端设备状态和IP使用状态，页面展示主要包括终端列表、IP管理、终端扫描设置等。

配置思路：

管理员启用全网终端监控的配置逻辑：先启用发现设置，根据需求选择配置监控网段，完成配置后，终端列表页面才会显示终端资产信息，然后通过IP管理可查看内网存活IP情况。

发现设置

终端识别设置中的监控网段是指通过被动流量（流量需要经过AC或镜像流量到AC）来识别资产终端类型的识别范围。

步骤1.在[全网监控/全网终端监控/发现设置]，监控网段页面勾选启用全网终端识别功能。

步骤2.配置监控网段，该网段会被动进行识别，并且将IP信息呈现在IP管理中。

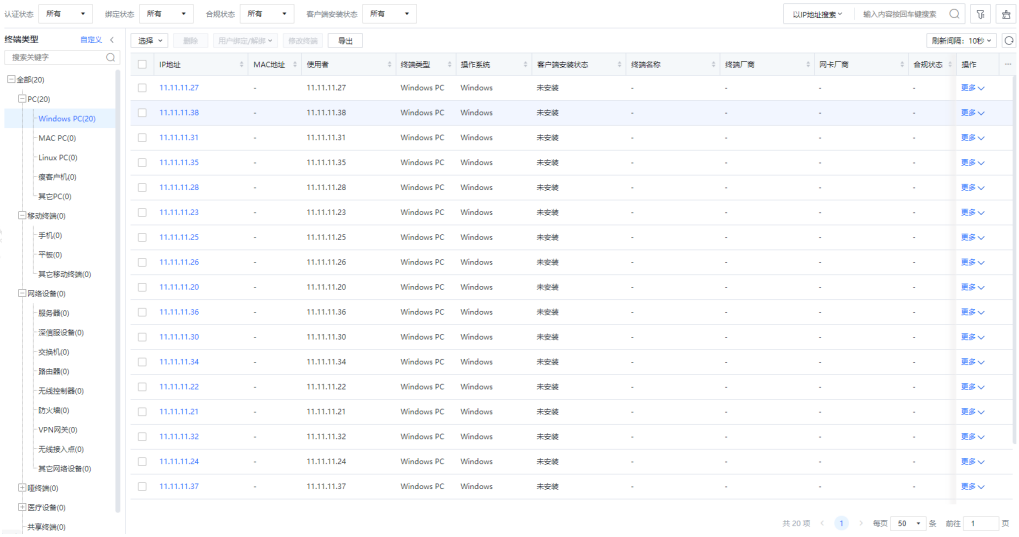
步骤3.根据需求是否要勾选<自动删除长久未发现的终端>，默认天数为180天。

步骤4.点击<保存>，完成终端识别设置。

终端列表

终端列表主要用于查看内网终端设备情况，未启用终端扫描的情况下的页面如下所示。

点击<立即启用>，跳转到终端扫描设置界面，完成配置后显示终端列表页面，在资产网端配置内网的网段。



（可根据认证状态、绑定状态、合规状态、客户端安装状态、在线状态、冻结状态、客户端版本、首次发现时间、操作系统、IP地址进行筛选）。可根据需求对单个IP/MAC加入用户绑定，修改终端类型。

在组织结构页面中可进行设置和过滤需要显示IP和相应的状态，同时也能对终端用户进行绑定操作；终端列表可根据需要显示进行选择，其他功能参数如下表说明。

表5终端列表操作说明

操作	功能说明
自定义	自定义终端类型，能新增，也可以删除、上移、下移操作；当终端同时符合多个终端类型的判断条件时，按列表优先级较高>列表优先级较低>内置终端类型的顺序进行判断。
选择	可选择当前页面和所有页的IP地址，然后再进行其他操作。
删除	选择需要删除不需要的IP地址或者用户。
修改	选择需要修改的终端，可更改终端类别和类型，并且备注终端厂商。也可点击<恢复默认

终端类型	失败结果>可恢复到最初的识别情况。
用户绑定/解绑	可单个用户绑定和批量用户绑定，可绑定目的、绑定对象、绑定有效期；且当使用者为空时可选择IP地址或者MAC地址来绑定。当不需要绑定时，选择已绑定的用户点击解绑即可。
导出	选择部分IP地址或者全部终端列表的IP地址数据到本地。
认证状态	可选择所有、已认证、未认证、认证失败等进行过滤显示。
绑定状态	可选择所有、已绑定和未绑定来过滤显示。
合规状态	可选择所有、合规、违规、异常来过滤显示。
客户端安装状态	可选择所有、已安装和未安装来过滤显示。
搜索	可根据IP、IP段、MAC地址、使用者来搜索过滤显示。
更多筛选	过滤条件设置可根据在线状态、冻结状态、客户端版本、首次发现时间和操作系统等来过滤显示。

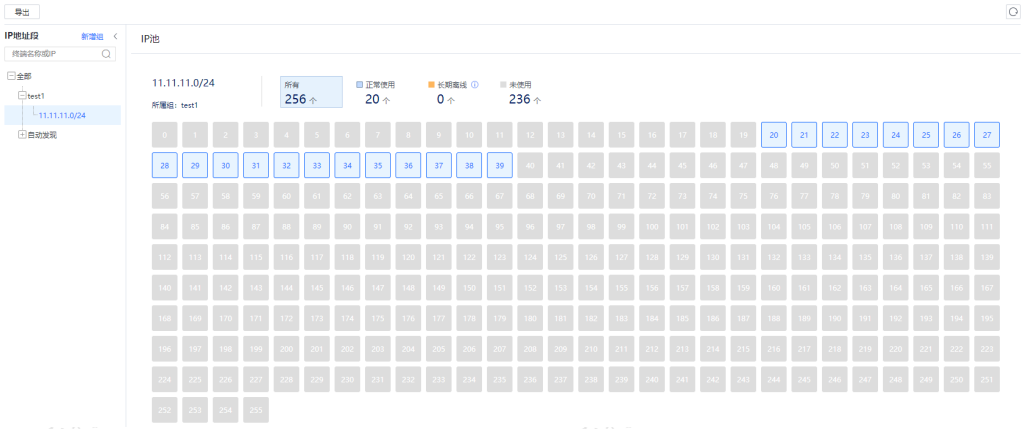
点击资产IP地址可以查看到终端的详细信息和认证信息，如下图。

详细信息说明：

1. 客户端版本分为最新和非最新，最新的则为当前版本对应的客户端版本。
2. 在线状态：在线指在线用户信息中是否有该终端的IP，有该IP说明有用户使用该终端上线了，同时会显示使用者信息和所属组的状态。离线指该终端IP目前没有用户使用。

IP管理

通过IP管理查看内网存活IP情况，IP地址段可实现内网存活的IP地址所在的24位地址段，最大显示1024个C段，右边显示段内具体存活情况,当鼠标停留在IP图标上会显示IP当前的信息状态。



正常使用：一段时间（默认是30天，支持自定义配置）内AC设备有收到过该IP所发出的数据包且这段时间内有终端用户使用该IP在AC上完成认证上线，则判定为该IP为“正在使用”。

未使用：指AC设备从未接收到此IP所发出的流量信息。

长期离线：指该IP之前被AC设备判定为“正常使用”后连续一段时间（默认是30天，支持自定义配置，鼠标停留在长期离线后的“小i”按钮，可对连续时间进行设置）未再识别到该IP所产生的流量则定义为长期离线。

IP段呈现机制：IP段列表中只有扫到有存活IP时才会显示该IP所在24位掩码的网段，或者该IP有流量过AC时该IP所在24位掩码的网段也会显示。

表6IP管理操作说明

操作	功能说明
立即刷新	点击<立即刷新>立即刷新当前所有的识别IP地址段。
导出	可选择所有IP 或者某个组和自定义范围的IP 导出到本地。
新增组	新增自定义的组，必须要选择一个IP地址才能添加成功，不能新增空组。
置顶	选择需要置顶的组点击置顶可置顶在第一的位置，选择某个组的IP点击置顶，可置顶到当前组最前面的位置。其中自动发现组不能置顶操作。
编辑	选择需要编辑的组，可进行编辑组、解散组和取消置顶；选择需要编辑的IP，可进行编辑备注、移到组和置顶操作。

合规检查状态

合规检查状态主要是检测到所有终端的合规状态，也可以根据生效状态和规则名称进行筛选展示，该章节显示的数据需要在终端检查章节进行配置策略，当设备检测到PC有不合规的行为的结果都会在该列表显示。

点击<过滤条件>可以设置指定的条件查看相应的用户。过滤类型有组过滤、用户过滤、IP过滤，填写完成点击<提交>即可。

其中：

- 组过滤：**可以根据组织架构进行选择。**
- 用户过滤：**可以通过用户名进行过滤，一行一个用户名。**
- IP过滤：**勾选后可以输入IP地址进行过滤。**
- 生效状态：**可选所有、违规、合规、异常。**
- 规则名称：**可根据规则名称进行搜索违规情况。**

流量状态

流量状态用于显示设备的在线用户的流量信息、各个应用的流量信息、流量管理的通道状态信息、用户配额状态等信息，包括用户流量、应用流量、业务流量排名，流量管理状态、链路负载状态、用户配额状态。

用户流量排名

管理员可在[全网监控/流量状态/用户流量排名]页面查看用户使用带宽的情况和进行相关的管理操作。

根据用户上行和下行流速进行排名。显示内容分别包含：用户名、所属组、上下行流速、总流速、会话数、是否冻结上网、获取机器名和流量构成。

表7用户流量排名管理操作

操作	功能说明
刷新间隔	用于设置页面上排行刷新的时间间隔
冻结用户	点击<冻结用户>用于立即断开某个用户连接，使其无法上网一段时间。
解冻用户	当需要被冻结的用户解开限制，点击<用户列表解冻用户>，会跳转到在线用户管理，找到被冻结的用户，选中该用户点击<解冻>即可。
过滤	点击<过滤条件>，可以设置具体用户排名来过滤。 过滤类型：包括查看的线路和应用。过滤对象：用来设置具体的用户或者IP，组过滤、用

条件	户过滤、IP过滤只能三选一。 显示选项：可设置流量排名前多少名的用户。

应用流量排名

管理员可在[全网监控/流量状态/应用流量排名]页面查看设备实时的应用服务的流量排名情况和进行相关的管理操作。

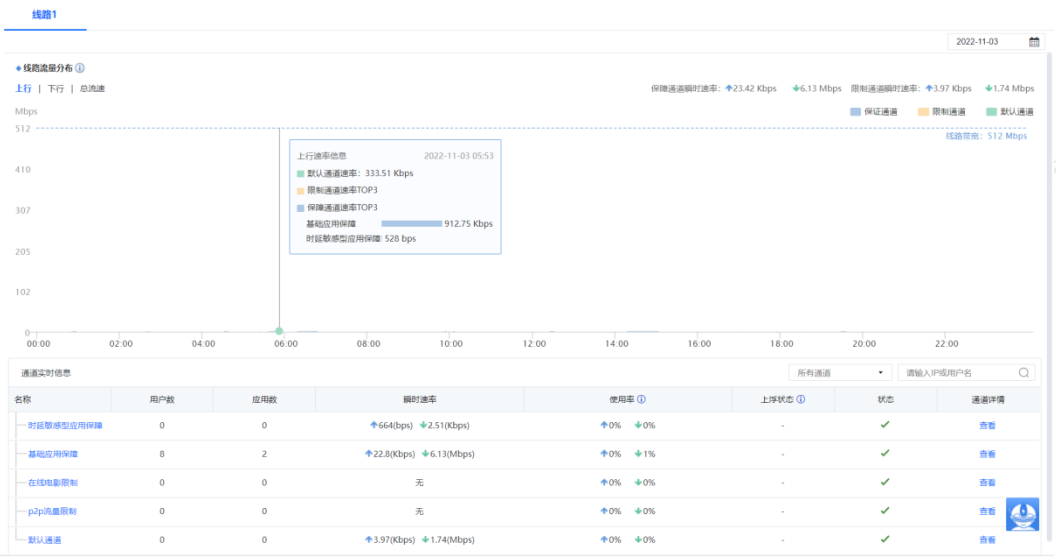
根据应用占用的带宽进行排名，看到的内容包括：应用类型、上下行流速、总流速、线路、占用带宽的百分比以及应用流量的主要用户构成。

业务流量排名

管理员可以显示当前业务流量情况，包括业务的IP端口、上下行流速、连接数、访问用户、具体内容可以通过点击详情进一步查看。

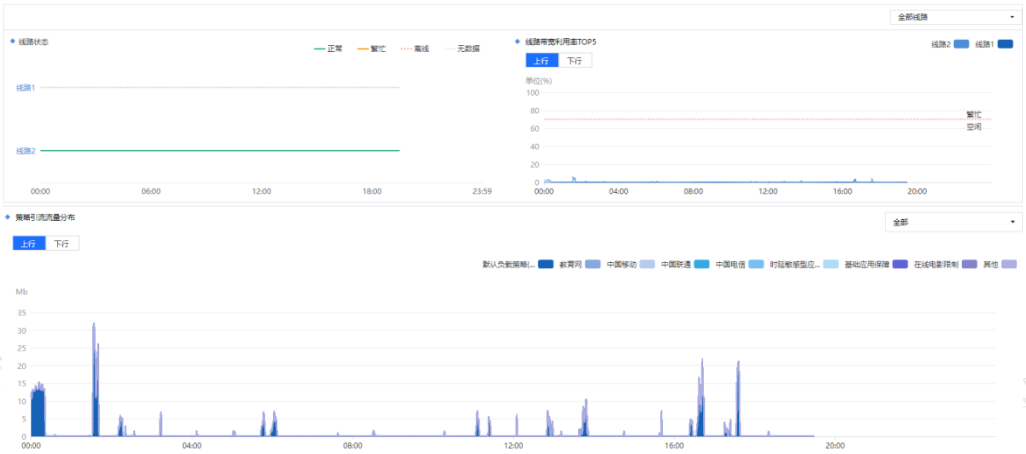
流量管理状态

流量管理状态是用来看流量管理设置通道流量信息，有线路一和线路二的流量，前提条件是流量管理已经启用了流量管理的通道，界面如下。



链路负载状态

链路负载状态可展示当前链路状态情况（正常、繁忙、离线、无数据），链路带宽利用率TOP5(上行、下行)的情况，以及策略引流流量分布情况。



管理员还可以查看策略引流实时信息，包括实时和当天累计牵引情况。

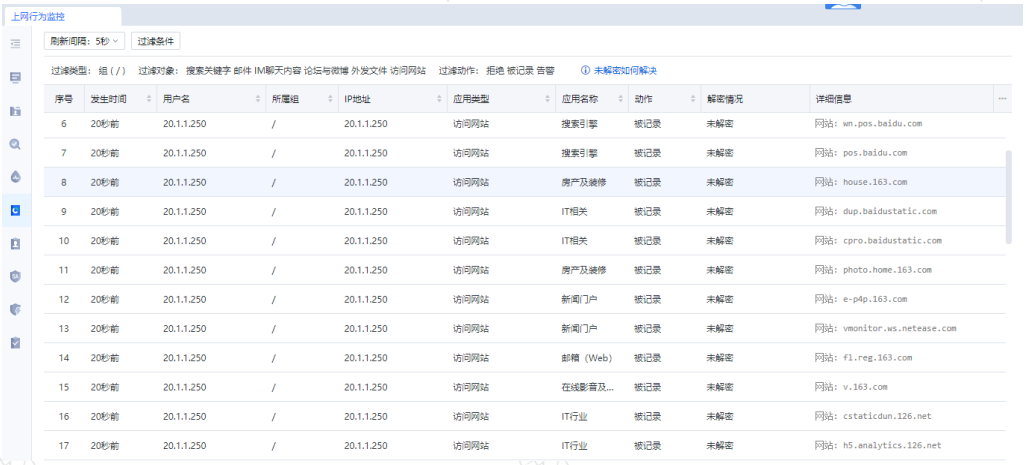
管理员可点击任意策略名称或详情，可跳转到策略详细信息说明。

用户配额状态

用户配额状态是用于查看指定的用户或者配额策略的使用情况，并可以进行重置操作。该功能生效的前提条件需要在[流量管理/用户限额策略]配置并启用。管理员可以根据按配额策略查询和按用户查询设备的使用情况，还能通过每日流量、每月流量、时长来重置相应的情况。

上网行为监控

管理员可对所有用户上网的行为进行监控和过滤需要查看用户的类型、对象和动作。



此处可以看到对应用户的上网行为、发生时间、IP地址、应用类型、应用名称、动作、解密情况和详细信息等。

用户点击<过滤条件>，可设置需要查看的行为，其中包括过滤类型、过滤对象、过滤动作。

过滤类型：设置需要查看的用户，可以在组过滤、用户过滤和IP过滤中选一个进行设置。

过滤对象：设置需要查看的行为，有搜索关键字、论坛与微博、邮件、外发文件、访问网站和其他可供选择。

过滤动作：设置需要查看的动作，有拒绝、被记录、告警可供选择。

受惩用户列表

管理员可以查最近上网受惩罚的用户。首先需要配置并启用[策略管理/上网策略/用户限额策略]，配置了惩罚手段。然后用户列表会显示对应用户的惩罚详情、操作、发生时间、IP地址、违规类型、受惩罚剩余时间等。

立即解除：选中指定的受惩用户，点击<立即解除>可以解除惩罚。

解除所有用户：点击<解除所有用户>，所有惩罚用户都将被解除惩罚。

点击<过滤条件>，可以设置具体需要查看的惩罚条件，其中过滤对象用于设置需要查看的用户，可以在组过滤、用户过滤和IP过滤中选一个进行设置，处罚来源有流量超额、时长配额、流速限制、连接数超限。

SaaS应用分析

随着互联网的兴起，从Web2.0到Html5.0的演进，越来越多的软件提供商提供SaaS服务，承载着用户对互联网的使用，它带来便利性也同时造成影子IT的风险。

“影子IT/Shadow IT”定义：所有的没IT组织参与的应用，以及没有被IT服务管理覆盖的应用，都在影子IT的范畴内。

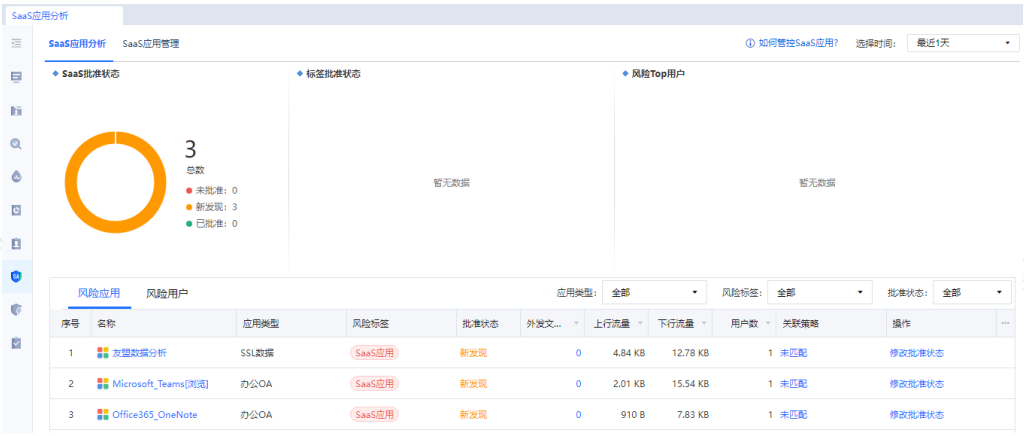
影子IT带来隐藏的风险和成本，大企业网络里面可能运行着成千上百的云应用，其中大部分是影子服务，这类服务由于使用不受IT监管，对数据和业务可能构成较大的风险以及引发合规问题，所以如何治理影子IT，变成企业信息安全亟待解决的问题：

- 如何检视和评估SaaS应用的使用
- 如何发现与治理隐藏的影子IT风险

• 如何管理SaaS应用

为了能掌握企业内部的应用使用情况，管理员通过设备类型识别对这些应用做SaaS定义，可对这个某个应用设置允许使用或不允许使用。

使用方法可直接点击<如何管控SaaS应用>，会有详细的操作指南。



点击<风险应用>，就会显示应用名称、应用类型、批准状态等信息，未批准的状态都是显示新发现，关联策略如未匹配，可点击<未匹配>跳转到权限控制策略进行设置相应的权限。批准状态可选择允许和拒绝是否可用。

管理员还可以在[行为管理/访问权限策略]，点击新增访问权限策略中的应用控制类别中的SaaS高级选项配置包括Google、Youtube、Office365、Bing Search、Facebook、Dropbox等进行细化行为管控设置。上述功能需要开启SSL解密策略才能支持。

安全状态

安全状态主要用户显示设备检测到不安全的行为，分析风险用户和安全事件。其中包括分析用户、安全事件、热点事件。也可开启深信服云脑功能，如已经开启，点击<已接入深信服云脑>可直接跳转到安全能力的云脑界面。

风险用户：红色表示用户已被感染，橙色表示用户可能被感染。

安全事件：可以显示僵尸网络、恶意链接、防内网DOS攻击、SAVE杀毒的安全事件

热点事件：接入深信服云脑，获取到热门安全事件top10，如果用户已经有发生，云图会变成红色，可点击查看详情。

筛选：可筛选安全事件类型，根据风险等级进行筛选。

过滤：可在输入框输入用户名或IP地址过滤需要关注的用户。

详细信息列表：可以查看具体风险用户和具体安全事件。

点击<风险用户>进入风险用户列表页面。

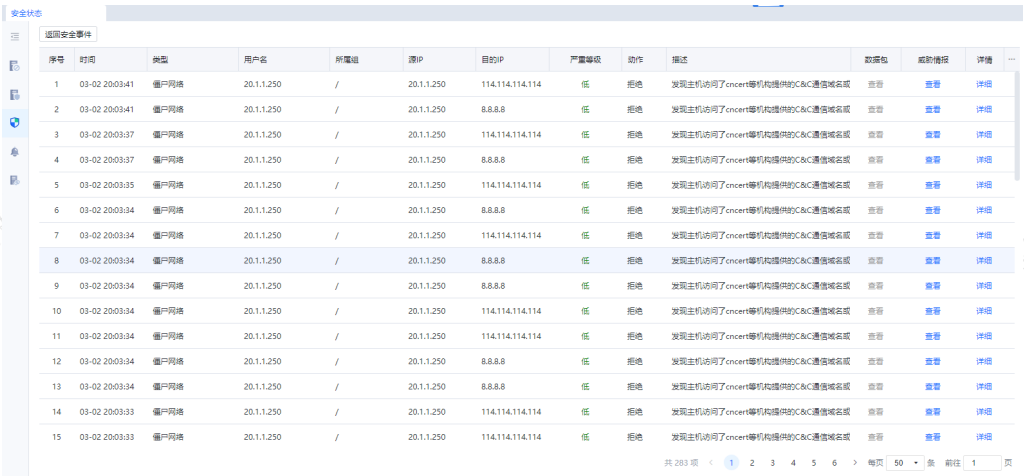
可选择指定用户点击<详细信息>，能看到安全事件发生的时间、攻击类型、详细描述信息、数据包、威胁情报等。

点击<详情>可显示如下信息。

时间：	03-02 20:03:41
用户名：	20.1.1.250
所属组：	/
协议：	UDP
URL/目录：	-
源IP：	20.1.1.250
源端口：	7908
目的IP：	114.114.114.114
目的端口：	13568
严重等级：	低
动作：	拒绝
描述：	发现主机访问了cncert等机构提供的C&C通信域名或IP，域名为：bitclockers.com，IP为：114.114.114.114，可能感染挖矿类别病毒或minepool家族病毒

点击<安全事件>进入安全事件页面。

点击<日志>跳转到安全事件详情，可以查看数据包、威胁情报和详细信息等。



审批中心

审批列表主要是用来显示自注册用户的信息，其中包括申请时间、申请类型、用户名、用户组和账号有效期等，管理员可在审批列表审批。

管理员在拒绝用户的自注册申请时，会出现审批意见框用于备注拒绝原因，同时记录到审批历史记录，用户使用拒绝账号登录时会提示审批拒绝以及原因，这个审批意见允许不填，支持批量审批只填1次意见。

接入管理

接入管理的作用是管理内网用户、配置内网用户的认证方式。其中包括用户管理、接入认证、终端检查。用户管理主要是对内网用户统一管理和配置，接入认证主要是可配置内网用户的认证方式、认证服务器。终端检查是实现对终端的合规性和非法外联的管控。

用户管理

用户类型

全网行为管理设备上的用户类别分为三类：本地用户、AD域用户、临时用户。

本地用户：可以直接通过[用户管理/本地组/用户]的页面进行管理和配置的用户。添加本地用户的方式包括：

- 管理员在[接入管理/用户管理/本地组/用户]创建；
- 通过[接入管理/接入认证]设置，认证后自动添加（包括不需要认证、通过第三方认证服务器认证、单点登录都可以设置成自动添加到本地组织结构）；
- 通过导入功能导入；
- 通过[用户管理/用户自动同步]功能同步到本地。

AD域用户：内网需要有AD域，AC需要结合AD域用户作为第三方认证和单点登录认证时，AC设备会实时获取域用户及组织结构，并和AD域结构保持完全一致。可直接在用户组进行管理。由于部分用户并没有同步到AC本地，所以在AC设备上对这部分用户无法进行删除和移动操作，只能对这部分用户关联权限策略和流控策略等。

临时用户：是通过AC认证但是没有加入到AC组织结构的用户，这部分用户不会显示在[本地组/用户]的页面。配置方式在认证策略中指定，[认证后处理]中的“非本地/域用户使用该组上线”中选择对应的组，临时用户就匹配这个组的相关策略。

本地组/用户

本地组/用户可以管理和配置AC本地用户组和用户，还能对用户组和用户进行新增、删除、批量编辑、导入导出、移动用户的操作。

新增组/用户

新增子组

设备会默认自带的组为root组（根组），该组不能删除，组名也不能修改。新增的组都是root组的子组。根组是一级组，根组下新增的组是二级组，依此类推，本地组最多支持16级组织架构，包括根组。这样的设计更符合公司的组织架构，方便管理。例如：在根组下新增一个工程师组。

步骤1.在本地用户中选择需要添加子组的用户组，右边进入管理界面。在成员列表点击<新增>按钮，然后选择新增类型“组”。

步骤2.设置组名列表的名称“工程师”和描述信息。

步骤3.配置完成，点击<提交>，在成员列表就可以显示子组的添加。

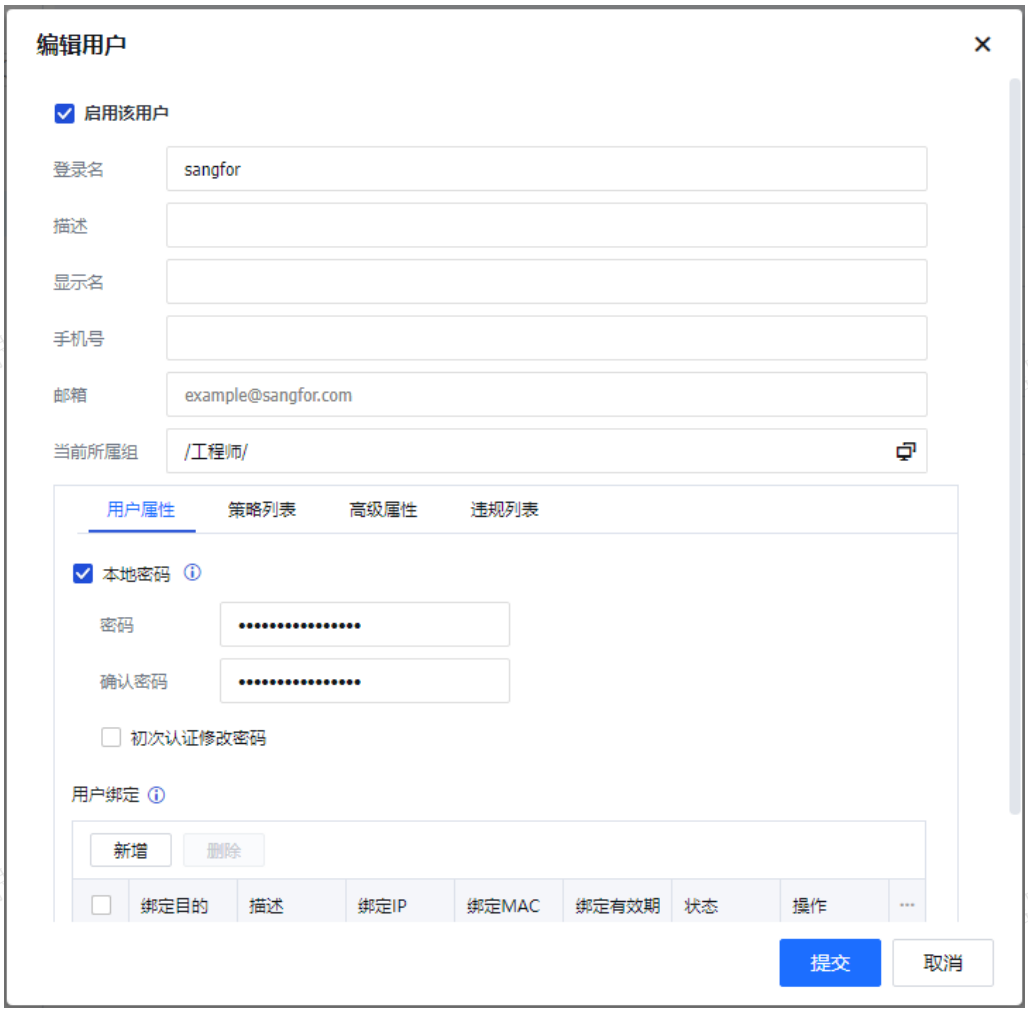
步骤4.添加子组成功后，可在该组下导入属于该组的用户信息，或者新增用户。

新增用户

新增用户主要分为两种方式：普通用户和多用户。管理员可以新增用户信息，用户可以通过密码认证的方式

接入网络。

步骤1.在[接入管理/用户管理/本地组/用户]，在成员列表，点击新增选择用户。



步骤2.管理员在勾选<启用该用户>，填写登录名（必填项），描述、显示名、手机号、邮箱（非必填项，根据需求填写），当前所属组可把新增加的用户放到对应的组里面。

步骤3.管理员设置用户属性，勾选<本地密码>，设置登录密码，如果该用户使用外部密码认证时不需要勾选。

步骤4.管理员可在策略列表显示当前配置的策略，创建新策略或者移除策略。在高级属性可设置密码认证成功后注销窗口、允许多人同时使用该账号登录、允许修改本地密码，如想限制部分IP登录，可以勾选“限制以下地址范围内登录”，然后填写需要限制的IP地址。违规列表可显示该用户的合规检查信息（终端检查策略）。

初次认证修改密码：是强制要求用户在初次认证通过后，修改初始密码，当用户为公共账户（即允许多人同时使用该账号登录）时，[初次认证修改密码]选项不生效。

步骤5.管理员点击<新增>用户绑定，可绑定IP、MAC信息。

新增用户绑定：用于设置用户IP和MAC的绑定关系。填写描述、绑定目的、绑定对象、绑定有效期，绑定目的可选：免认证、限制登录、免认证且限制登录。在绑定对象填写绑定的IP和MAC。

- 免认证：**用户认证后，不需要每次都做认证；**
- 限制登录：**用户只能在某个范围内进行认证，认证范围指的是绑定对象；**
- 免认证且限制登录：**用户只能在某个范围内认证，且认证后在免认证有效期内不需要每次都做认证。**

步骤6.点击<提交>完成用户的添加，在成员列表会显示出刚创建的用户。

步骤7.创建成功后，即可通过本地密码认证方式输入账号（张三）和密码来认证上网。

新增多用户

- 新增多用户用于同时新增多个用户，与新增用户不同的是，新增多用户时不能设置高级属性中的[终端绑定]，即IP、MAC绑定。因为这一项设置具有唯一性，不能在添加多用户时设置。
- 新增多用户设置的多个用户的属性和策略是完全相同的，除了用户名。在用户名列表中配置多个用户名，用户名之间用英文逗号隔开，新增多用户时，因多个用户初始密码是一致的，可以设置要求用户初次认证时必须修改密码，其他配置和[新增单用户]相同，可参考新增用户章节。

组/用户管理

管理员可对用户组和用户进行新增、删除、批量编辑、导入导出等操作。

表8组/用户管理功能说明

操作	功能说明
删除组/用户	把不需要的组或用户删除。选中需要删除的[组/用户]，点击<删除>即可。当[认证策略]关联了需要删除的用户组，则此用户组将无法直接删除，需要先删除认证策略，才能将该组删除。
编辑/批量编辑	批量编辑与单用户编辑的不同在于可编辑的属性不同。批量编辑，可以针对多个用户或多个组进行编辑，批量编辑用户时不能设置高级属性中的终端绑定，即IP、MAC绑定。因为这一项设置具有唯一性，不能编辑多用户时设置。
导入/导出	将组/用户的数据批量导入或者导出设备。通过CSV文件导入方式，导入用户时可以同时导入显示名、所属组、密码、允许登录的IP范围、是否公用账号、自定义属性等。如果导入用户时指定的所属组不存在，也会自动建立用户组。 勾选需要导出的组和用户，以CSV文件方式导出。当某个用户组没有用户时，此用户组不支持单独导出。
高级搜索	可以设置查询条件和范围：IP和MAC进行筛选，其他选项可以自定义查询。
上移/下移/移动到	AC本地的用户和用户组，支持移动。可以把现有的用户或者组，移动到其他组下。成功移动后，用户会从原来的组中移动到目标组中并且使用目标组的上网策略。
过滤	可输入需要过滤策略的名称，进行策略的过滤。

域用户

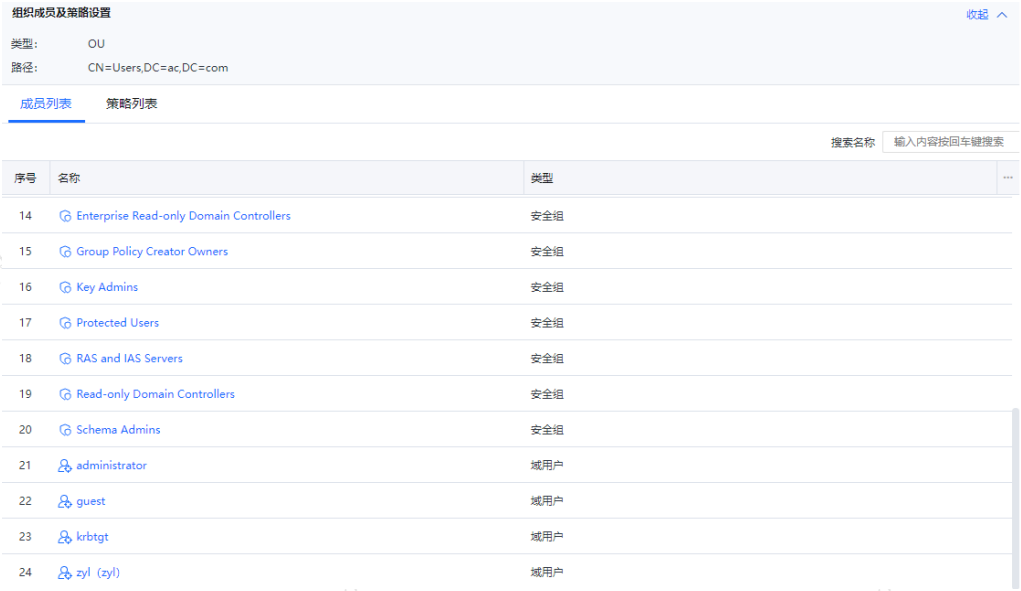
域用户是通过AD域服务器的目录数据库来存储的用户账号信息，可实现数据冗余和备份。规范网络架构，采用活动目录进行集中式管理。

AC从AD域服务器上实时获取到域用户，保持LDAP的组织结构，获取LDAP域组织结构的前提需要在认证服务器中将LDAP域服务器添加进去。

如果AC有结合LDAP域做认证，包括结合AD域做密码认证、AD域单点登录，那么在该页面就可以查看域用户和组织结构，以及关联的权限策略。

在组织结构中选择域用户，查看获取到的AD域用户和组信息。右边的组织成员及上网策略设置页面显示对应用户组的信息，包括：类型和组路径。

成员列表：页面中可以查看到各个组以及用户的详细信息。和本地账号的区别在于，域用户无法在AC上进行编辑、移动、删除等操作。



策略列表：用于查看对应AD用户组和策略关联域组织结构或用户的策略列表。

此处策略列表中的策略顺序和导航菜单策略页面中的策略顺序保持一致。因为策略的匹配是有顺序的，如果需要修改策略的顺序，请到策略页面，通过<上移/下移>按钮重新设置策略的顺序。

在策略列表中只能看到用户/用户组引用的策略名称，如果需要看到策略的详细设置还需要打开每条策略查看具体内容。策略结果集提供了一种方便的办法，便于管理员查看用户/用户组引用的详细策略。在策略列表页面点击<查看该组的策略结果集>，用于将某个组引用的策略整合起来，并且列出详细的设置。

用户绑定管理

用户绑定管理通常用于密码认证，也可以用于管理员定义了用户名的不需要认证场景。主要包括用户绑定、IP/MAC绑定、微信绑定。

用户绑定：当需要限制某个用户名只能在某个IP或MAC地址上登录，并且要求绑定的IP或MAC只能给这个用户使用时，需要用到用户绑定功能。

IP/MAC绑定：绑定用户的IP地址和MAC地址，可以方便管理员对内网用户进行统一管理，实现一人一机实名制管理。且将IP地址和MAC地址做双向绑定，即用户在认证时，会验证该用户的IP和MAC是否符合绑定的关系，如果有一项不对，就会认证不通过。为了防止内网有用户随意修改IP的行为。

微信绑定：将微信OpenID和用户信息绑定，实现微信快捷登录。用微信扫码实现密码登录，减去手动输入账号密码的步骤，其本质还是密码登录。账号可以是本地用户，域账号等外部账号。

动态令牌绑定：将动态令牌和用户信息绑定，实现用户通过动态码二次认证。管理员可配置用户动态令牌有效期为自定义天数或永不过期，以及是否自动删除过期绑定关系。

用户绑定

用户绑定的方式有自动录入和手动录入。

• 自动录入：**管理员在配置认证策略时的认证后处理选项勾选自动录入绑定关系-自动录入用户和IP/MAC的绑定关系，可以选择绑定IP、MAC、或IP和MAC，用户绑定支持设置有效期。**

• 手动录入：**管理员可在添加用户时绑定、用户绑定。添加用户时在[用户认证与管理/用户管理/组/用户]，可参考新增用户。用户绑定配置指导如下。**

步骤1.在[接入管理/用户管理/用户绑定管理/用户绑定]，点击<新增>跳转到新增用户绑定页面。

步骤2.勾选启用，设置绑定的用户名和描述，其中，用户名不仅可以对AC本地组织结构中的用户添加绑定关系，还可以对结合第三方服务器认证的用户添加绑定关系，如果这些用户是没有添加到AC的组织结构中，只要知道用户名，绑定关系仍然有效。

步骤3.选择免认证的绑定目的，包括免认证、限制登录、免认证且限制登录，勾选“免认证”。

• 免认证：**用户认证后，不需要每次都做认证；**

• 限制登录：**用户只能在某个范围内进行认证，认证范围指的是绑定对象；**

• 免认证且限制登录：**用户只能在某个范围内认证，且认证后在免认证有效期内不需要每次都做认证。**

步骤4.设置绑定对象：选择用户是绑定IP还是绑定MAC。

说明

：

在绑定MAC时如果管理员不知道该用户所用终端的MAC地址，可以点击<自动获取>输入该用户终端的IP地址后即可自动获取到MAC地址。

步骤5.设置绑定有效期：可以选择设置永不过期和过期时间。

步骤6.点击<提交>，用户绑定成功。

管理员可在用户绑定进行新增、批量编辑、删除、高级搜索、高级设置、选择、导入/导出。也可下载示例模板进行参考。其中：

批量编辑：用于同时设置多个绑定用户的描述信息和免认证设置。

高级搜索：用户可根据基本条件：用户名、IP、MAC进行搜索。根据绑定目的：免认证、限制登录、免认证且限制登录进行筛选。还可以通过加入时间和账号过期时间进行筛选列表中的用户。

下载示例模板：可以点击下载示例模板，根据提示和范例进行填写。

查看用户绑定错误报告：可查看认证过程用户绑定错误的报告。

高级设置：点击<高级设置>可跳到高级选项中，详情配置请参考高级选项中说明。

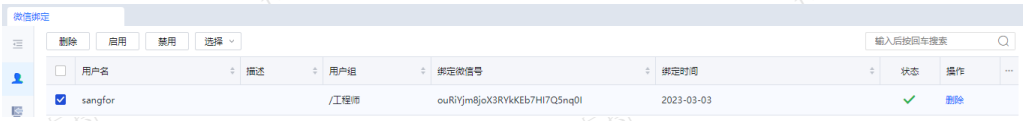
IP/MAC绑定

IP/MAC绑定的作用是为了批量导入，且将IP地址和MAC地址做双向绑定，即用户在认证时，会验证用户的IP和MAC是否符合这里绑定的关系，如果有一方不对，就会认证不通过。为了防止内网有用户随意修改IP的行为。

管理员可对相应的策略做删除、导入、导出操作，当列表策略较多，可以根据IP/MAC来搜索，也可以输入描述的信息，按回车进行搜索即可。

微信绑定

用户通过微信快捷登录后，将微信OpenID和用户信息绑定。管理员可对相应绑定信息做删除、启用、禁用、选择操作。



选择：批量选择绑定信息。

删除：删除绑定信息后，用户无法使用原绑定微信快捷登录，需要重新绑定。

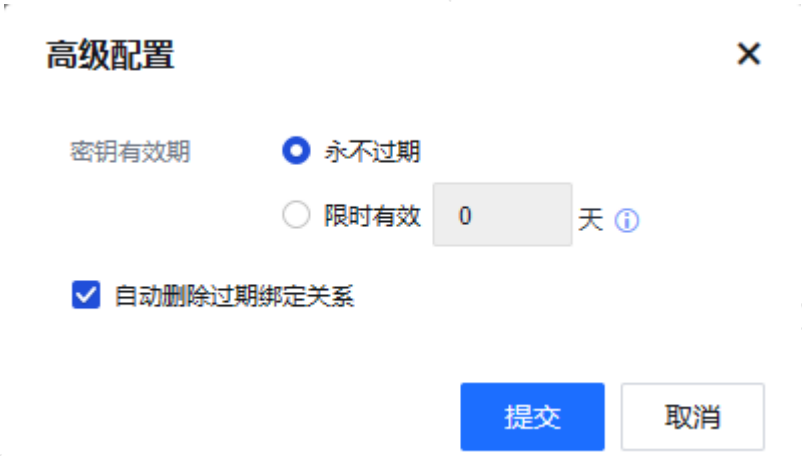
禁用：禁用绑定下信息后，用户无法使用微信快捷登录。

启用：对禁用的绑定信息启用，用户可以重新使用微信快捷登录。

动态令牌绑定

用户通过动态码二次认证后，将动态令牌和用户信息绑定。管理员可对动态令牌进行删除、搜索、排序等，如删除动态令牌绑定关系，用户需要在二次认证中重新绑定。动态令牌状态分为生效中、已过期和异常数据，管理员可点击二维码重新生成动态令牌，对生效中令牌重新生成，动态令牌不会重置；对已过期的动态令牌重新生成，会刷新生效时间，状态重新变为生效中；对异常数据令牌重新生成，状态重新变为生效中。

在高级配置中可对动态令牌绑定关系设置是否删除过期绑定关系和有效期，默认有效期为永不过期，也可自定义有效期为1-720天。



用户自动同步

当AC结合数据库或H3C CAMS或认证时，用户自动同步可将这两种系统上的用户数据同步到AC的本地组织结构。

在[用户管理/用户自动同步]，可对用户自动同步的策略进行删除、查看、立即刷新等操作。设备在每一次进行H3C CAMS同步时，都会产生一份同步报告，便于您查看同步的情况。点击<查看同步报告>，在同步报告页面选择对应的同步报告，下载后即可查看。

数据库同步

管理员将数据库中的用户和组同步到设备的本地组织结构中，可以进行自动同步，也可设置自动同步的时间间隔。

新增同步策略

同步策略用于设置数据库同步的相关参数，进行数据库同步时，是根据同步策略中的设置进行同步的。

步骤1.设置需要同步的数据库，设置IP、端口、登录用户名密码等信息，具体请参见[接入认证/PORTAL认证/认证服务器]（参见章节认证服务器章节）

步骤2.进入[用户认证与管理/用户管理/用户自动同步]，点击<新增>，在弹出的[数据库同步]窗口中设置同步参数。

步骤3.设置策略名称、策略描述，勾选[启用自动同步]设置自动同步的时间间隔，如图选择的是一天同步一次。

同步来源配置（远程）：选择第一步设置好的数据库服务器，填写可以获取用户的SQL语句和组路径分隔符，[组路径分隔符]用于数据表中以“组+分隔符+子组”的方式存储用户组名的情况下，指明以什么符号来分隔组和子组，如上述示例是以短横线“-”分隔，若字段中只包含一级组，没有子组，则此处留空。

同步目标配置（本地）：选择将同步过来的用户存放本地的组织结构中的路径。

勾选[同步到本地的用户默认允许多人同时使用该账号登录]表示同步到设备的账号默认是公用账号，即同一账号能够在多台电脑上登录，不勾选此项则表示用户是私有账号，只能同时在一台电脑上登录。

测试有效性：可以列出获取到的用户及所属组信息以及SQL执行耗时时间。

H3C CAMS同步

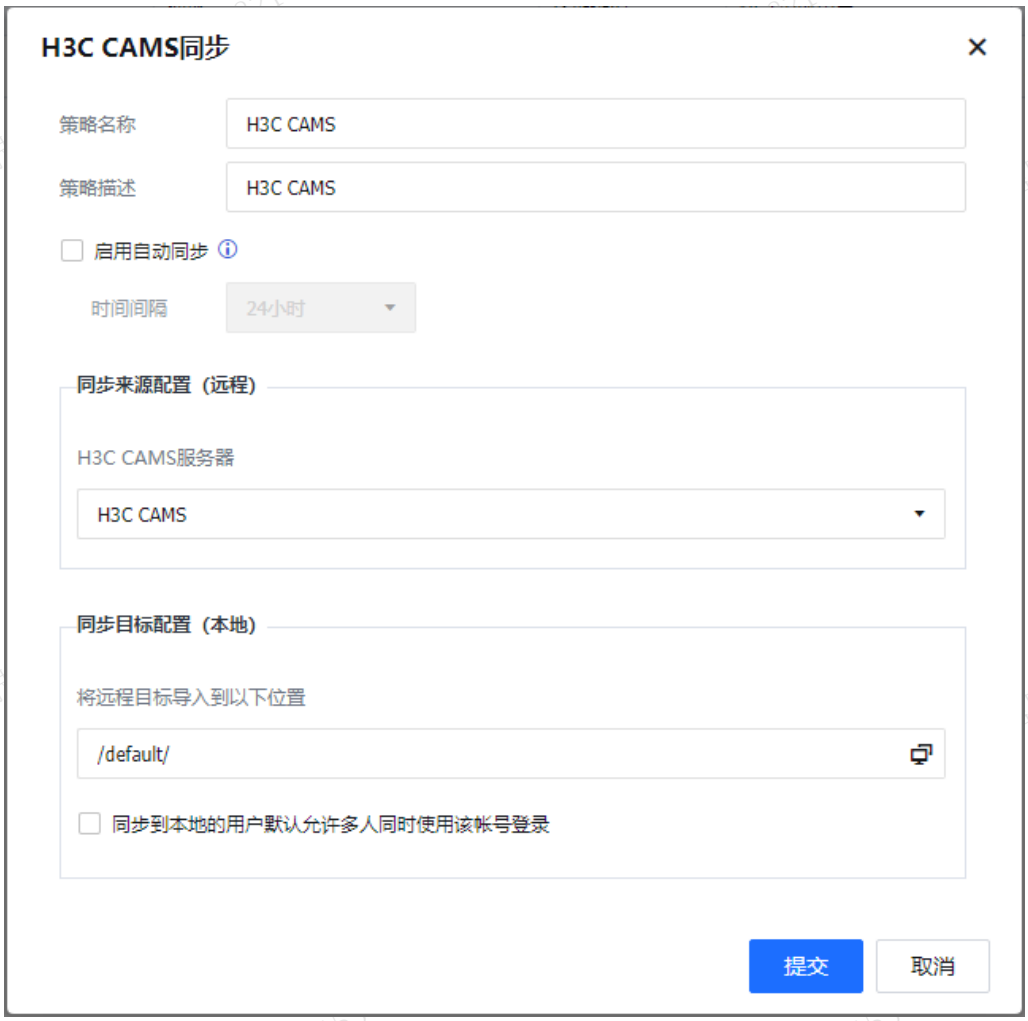
H3C CAMS是用于将H3C CAMS系统中的组和用户同步到设备的本地组织结构中，并且可以进行自动同步，可设置自动同步的时间间隔，实现对第三方平台组织结构中的用户，管理员也能进行关联策略。

新增同步策略

同步策略用于设置同步的相关参数，进行H3C CAMS同步时，是根据同步策略中的设置进行同步的。

步骤1.设置需要同步的H3C CAMS服务器，设置IP、端口、登录用户名密码等信息，具体请参见[接入认证/PORTAL认证/认证服务器]。

步骤2.进入[用户认证与管理/用户管理/用户自动同步]，点击<新增>，在弹出的<H3C CAMS同步>窗口中设置同步参数。



步骤3.设置策略名称、策略描述，勾选[启用自动同步]设置自动同步的时间间隔。

同步来源配置（远程）：选择步骤1设置好的H3C CAMS服务器。

同步目标配置（本地）：选择将同步过来的用户存放本地的组织结构中的路径。

勾选[同步到本地的用户默认允许多人同时使用该账号登录]表示同步到设备的账号默认是公用账号，即同一账号能够在多台电脑上登录，不勾选此项则表示用户是私有账号，只能同时在一台电脑上登录。

用户自注册

管理员出于工作目的期望获取入网终端的用户信息。如果用户信息全由管理员手动维护，不仅会增大管理员工作量，还会出现无法及时更新导致信息存在误差的情况。集中管理不如自我管理，深信服全网行为管理提出自注册和自管理的概念，实现账号自注册、终端自注册。

通过用户自助注册功能可实现用户自行注册，改变了之前只能由管理员手动创建的方式，减轻了管理员的负担，也方便集中管理。

注册方式

• 本地用户、外部密码服务器（包括微信/短信快捷登录）认证支持[账号自注册]。

• 当不需要认证但是期望录入个人信息帮助管理时，使用[终端自注册]。

• 其他认证服务器都不支持自注册，选择不支持的认证服务器，自注册功能会置灰。

配置思路

在配置认证策略时，提前定义好自注册相关信息，在认证策略时可直接引用。（本文已提前定义好自注册相关信息，认证策略可直接引用）。

一、账号自注册

账号自注册主要使用场景是在启用密码认证和外部认证服务器密码认证（包括微信/短信快捷登录）时，无需管理员手动创建，用户可以进行自注册。

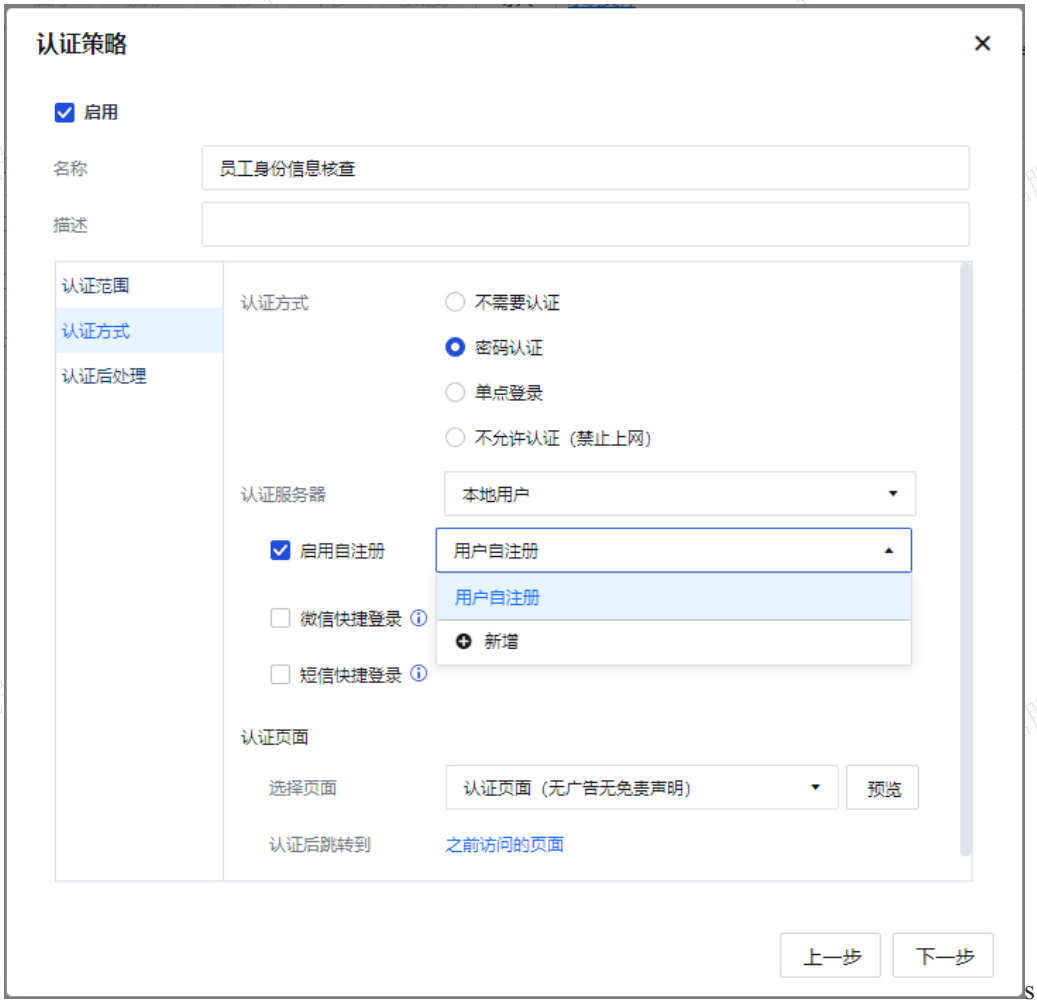
操作步骤

步骤1.在[接入管理/接入认证/PORTAL认证/认证策略]界面配置认证策略。

认证范围：按照实际需求填写认证范围。

认证方式：勾选密码认证，认证服务器选择本地用户。（目前仅本地密码认证支持用户自注册）

步骤2.勾选启用自注册并选择相应的自注册配置文件。如果未提前准备自注册配置文件，点击<新增>按钮添加用户自注册配置。其他功能项按需配置。



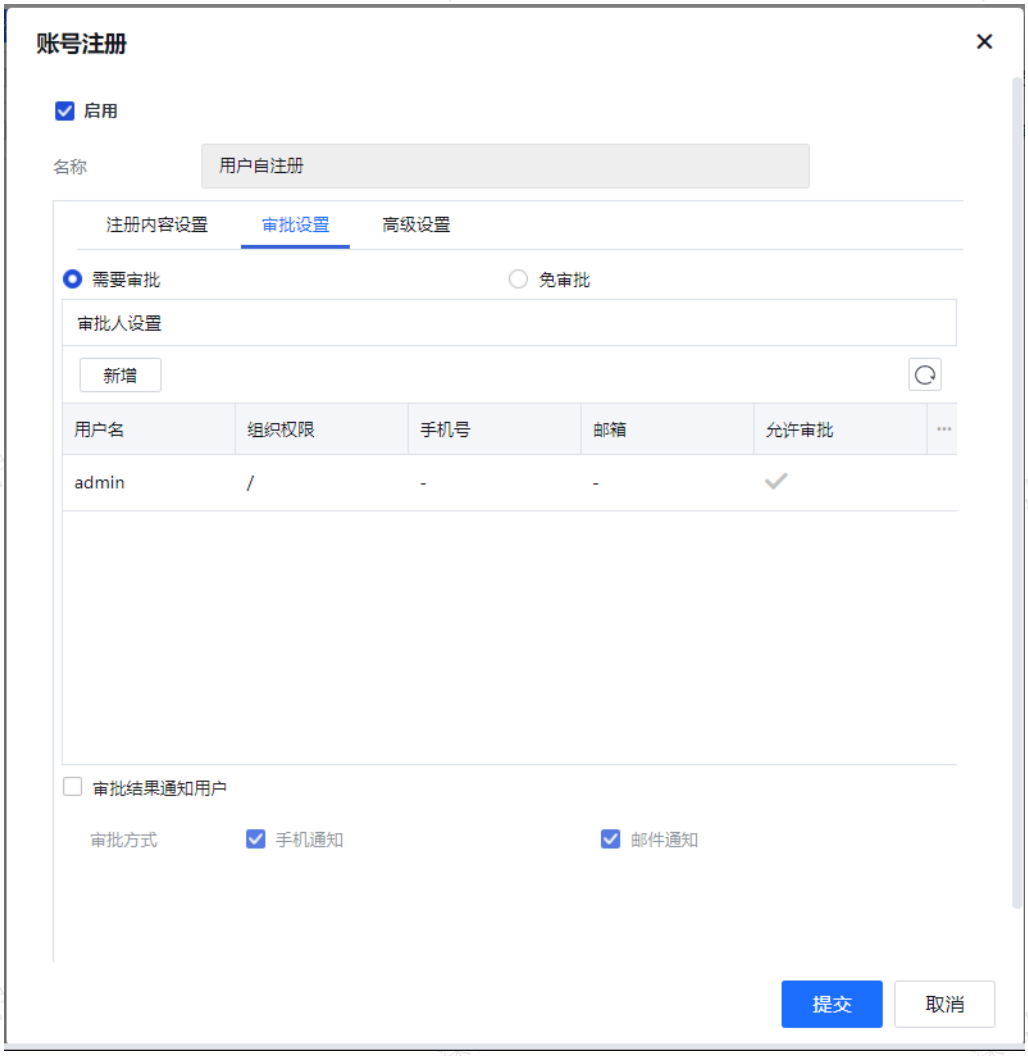
步骤3.添加用户自注册配置文件。在[接入管理/用户管理/用户自注册]界面点击<新增>按钮，选择[账号注册]。（终端注册适用于免认证场景）在名称：定义好文件名，方便后续管理。

步骤4.在[注册内容项]里点击<新增>按钮，可以添加访客需要填写的信息项。如需自定义内容项。

步骤5.请在[新增内容项]里点击新增按钮自定义信息项。

步骤6.在[审批设置]界面可以设置审批人。管理员可以在[系统管理/系统设置/管理员账号]添加一个审批专用账号。（该账号只拥有[审批列表]界面的读写权限）

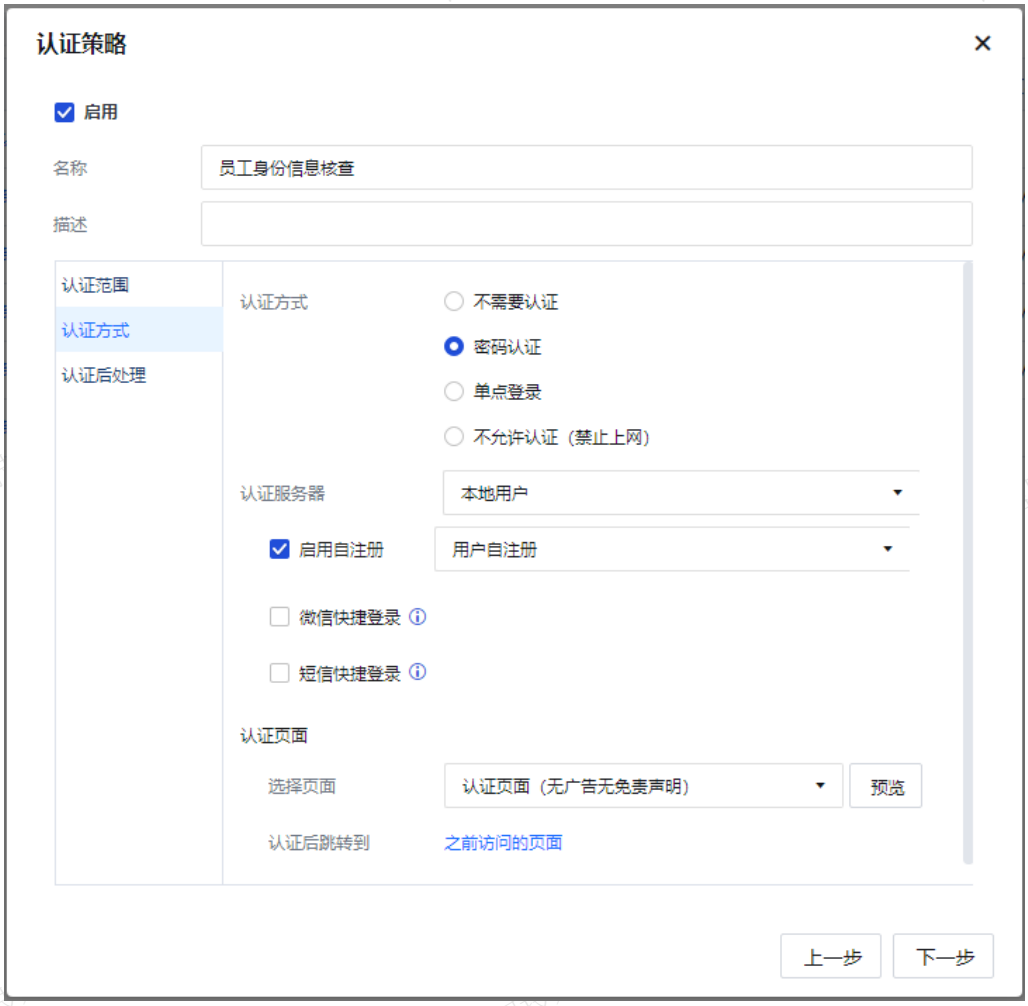
步骤7.审批结果可以选择通过短信或者邮件通知访客。（AC需要提前对接SMS平台或者邮件系统）。



审批结果通知用户：可以选择手机通知和邮件通知，需要提前保证通知可以用。

步骤8.在[高级设置]可自定义访客注册的账号的有效时间，也可配置用户名与IP/MAC地址绑定。

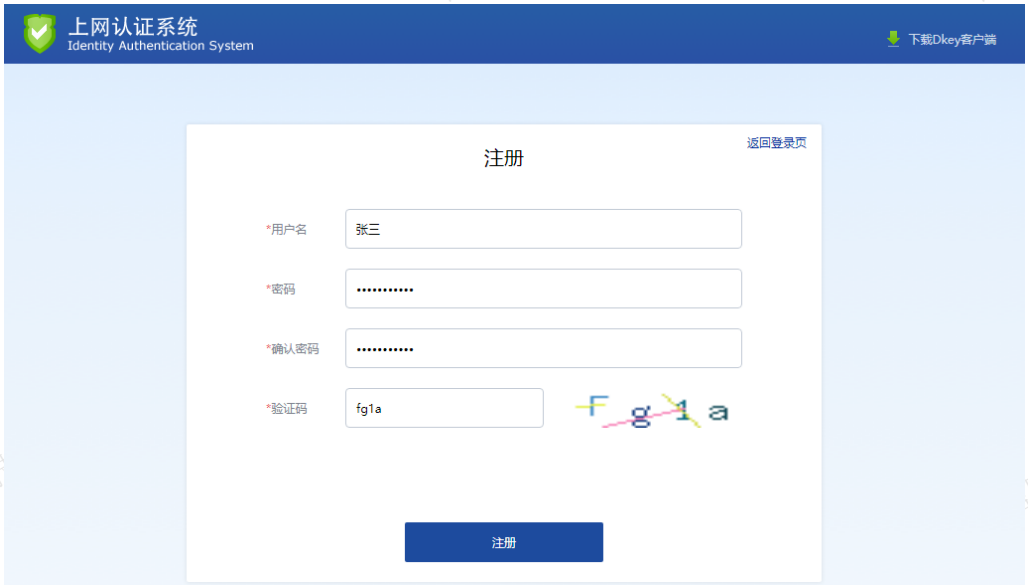
步骤9.提交启用了用户自注册功能的本地密码认证策略。



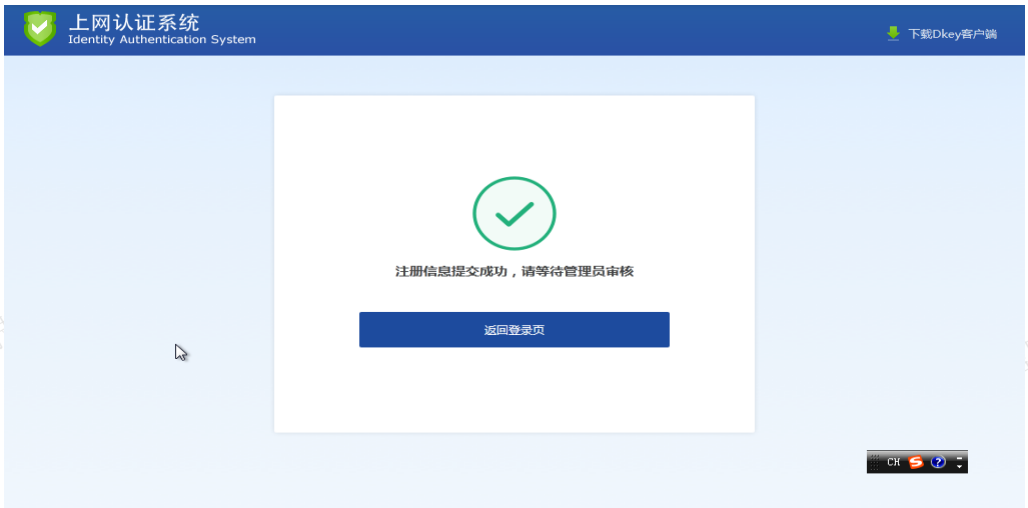
用户自注册流程：

步骤10.无入网账号的用户点击右下角的<注册>按钮，进入自注册流程。

步骤11.填写注册信息。在注册界面按照企业规定填写相关信息用于注册入网，点击<注册>按钮提交入网申请。



步骤12.当企业管理员审批完成后点击<返回登录界面>，使用自注册的账号登陆入网。



步骤13.管理员在[全网监控/审批中心]的审批列表里可以查看当前的访客入网请求。管d理员可以选择批准/拒绝访客的入网申请。

步骤14.当管理员完成审批后，访客使用注册信息完成登录。

二、终端注册

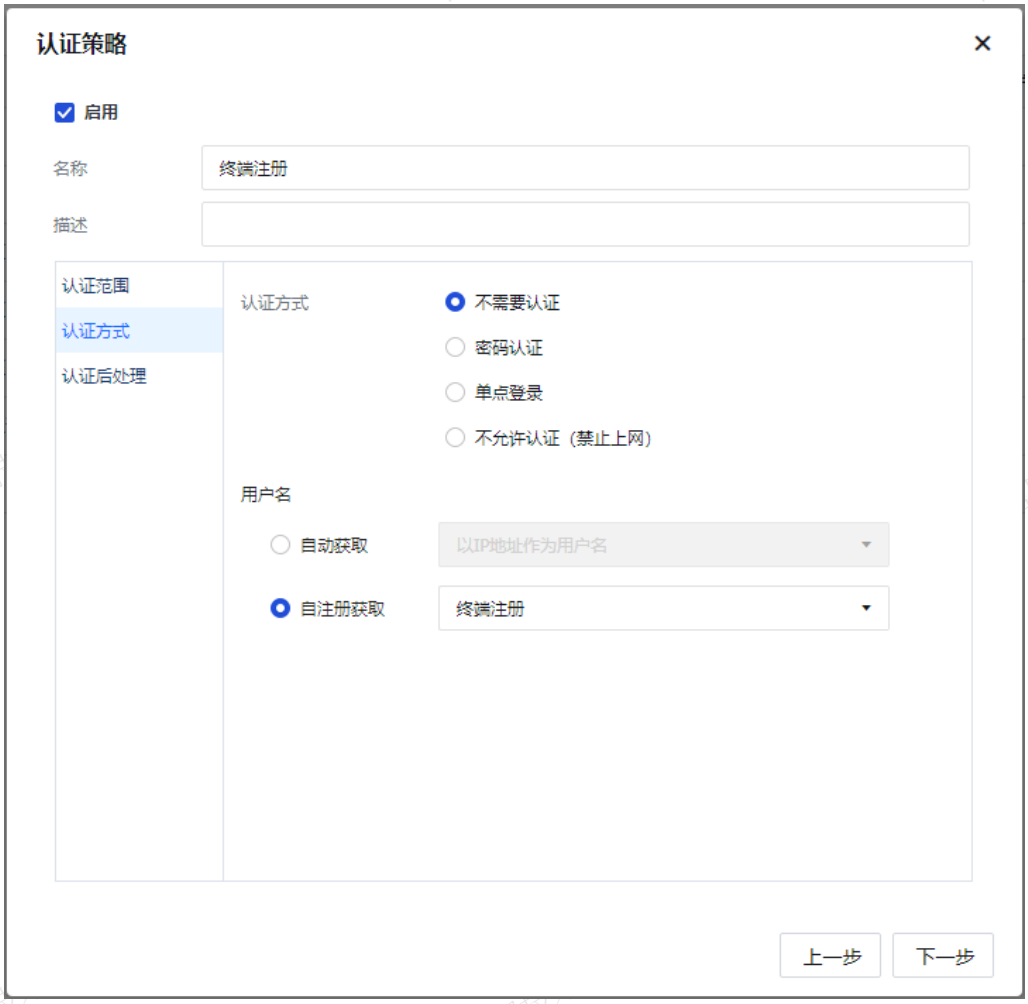
终端注册使用场景是在启用不需要认证时，期望入网设备录入个人信息，有利于企业管理员梳理网络资产。

步骤1.在自注册页面新增<终端注册>，注册内容设置、审批设置、高级设置方式和账号注册填写相同，在此

不在赘述。

步骤2.配置自注册认证策略，在[接入认证/PORTAL认证/认证策略]，新增自注册策略，填写名称和描述，填写范围。

步骤3.认证方式选择不需要认证，引用自注册获取后选择刚配置的终端注册策略，点击<提交>即可。



步骤4.效果呈现，访问网页会重定向到认证页面，弹出注册信息。

- 无需审批：**输入用户名，直接可以上网。**
- 需要审批：**输入用户名，等待审核结果，审核通过后可直接上网。**

开放接口服务

开放接口服务主要包括API开放接口和开放LDAP接口服务，设备本身提供服务。

API开放接口

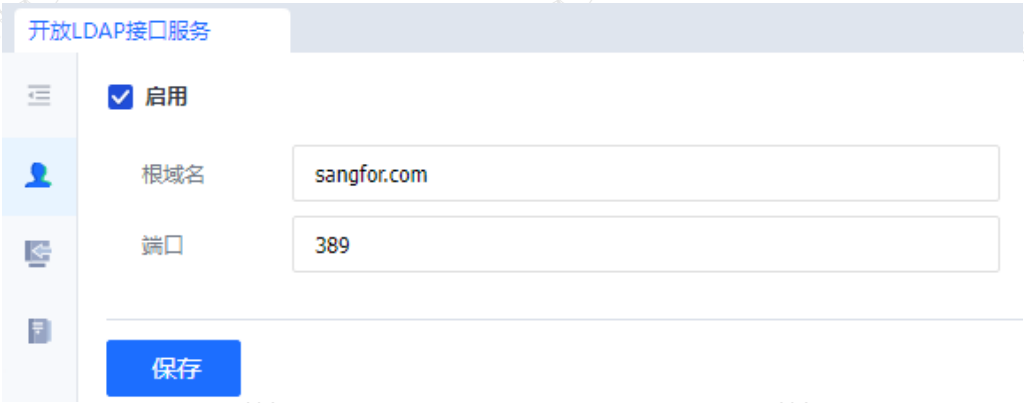
当第三方设备需要取AC设备的相关数据时，需开启API接口来实现，该接口类型为Restful接口，接口使用

方式请参考接口说明文档，可点击右上角[下载接口说明文档]。

在[接入管理/用户管理/开放接口服务/API开发接口]，勾选启用开放接口。

- 共享密钥：**用来校验对接的设备，双方共享密钥需保持一致。**
- 允许使用该接口的IP：**可配置允许哪些地址的服务器进行访问。**

开放LDAP接口服务



- 根域名：**在认证托管场景中，开启LDAP服务认证中心的本地用户会通过域用户方式存在于分支AC中。**
- 端口：**填写用于开放LDAP服务的端口，默认389，可自定义。**

说明：

1. LDAP接口服务是对外开放功能，用于对外开放LDAP服务。对外支持LDAP查询的用户信息包括：用户绑定信息、IP\MAC绑定、用户属性、本地组织结构，可用于认证托管场景。不支持通过LDAP接口查询其他信息，如用户所属的上网策略。

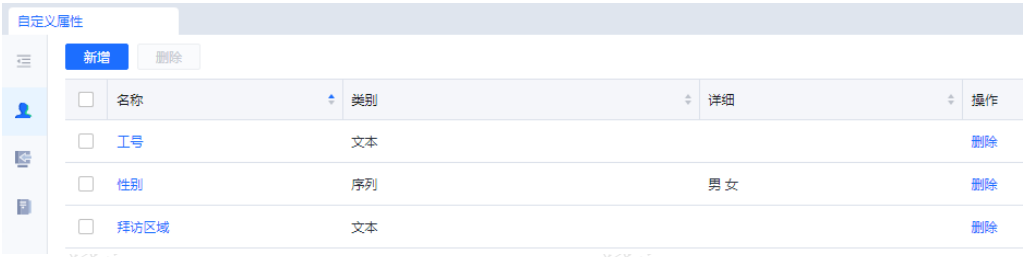
2. LDAP对外开放接口支持IPv6地址对接。

自定义属性

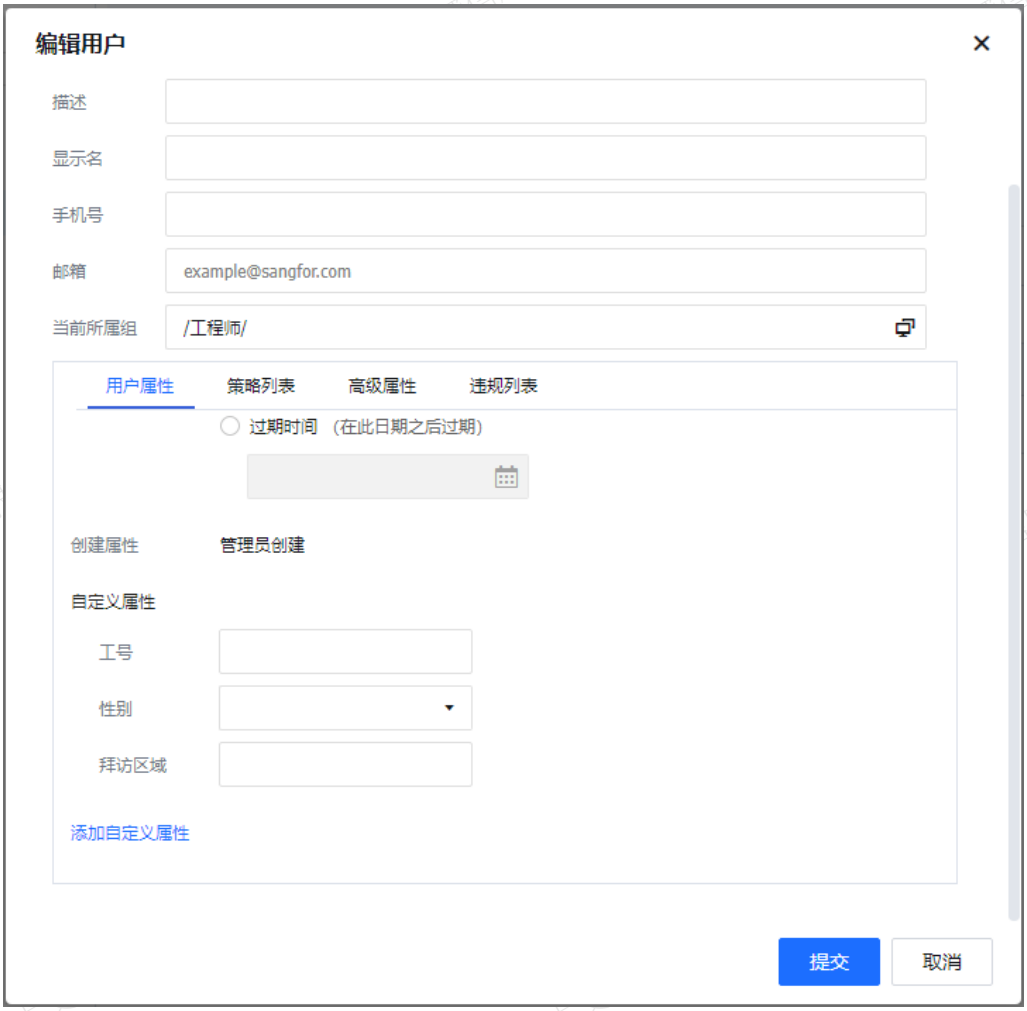
自定义属性通常在用户属性不满足设备权限管理需求时，管理员可以设置用户的扩展属性值。其中自定义属性的类别包括文本类型和序列类型。

• 如果类型为文本，则属性值可以在编辑用户的时候手动设置属性值内容。

• 如果类型为序列，则在此处设置几个序列值，比如属性为“性别”，序列值设置：男、女。编辑用户时可以选择属性值。



新增的自定义属性在本地组/用户在新增用户时引用。



接入认证

接入认证是用户入网的重要一步，只有完成了认证，才能基于用户配置相应的策略。

AC支持丰富的身份认证方式，提供了完善的认证体系，满足企业日常的认证需求。

目前认证主要分为两大类：802.1x认证和Portal认证，其中Portal认证可选多种认证方式，同时可灵活和第三方认证服务器结合。如下表所示。

表9认证方式场景说明

认证方式	认证服务器	场景说明
802.1X认证	-	802.1x认证结合交换机或无线控制器实现二层的管控，强管控需求可用802.1x认证。
不需要认证	-	终端用户以IP/MAC/计算机名为登录名，可自注册终端信息。
不允许认证		该认证方式禁止用户上网。
Dkey用户认证		用户通过key实现认证。
	本地密码	当用户名密码通过添加的方式存储在AC设备上时，可使用存储在AC设备本地的用户名密码实现本地密码认证。
	短信认证服务器	当存在短信网关或短信平台，可通过AC设备对接短信网关或短信平台，发送验证短信给用户，用户通过短信认证码认证上线。
	微信	

认证方式	认证服务器	当企业具有微信公众号时，可通过该认证方式，要求用户需要通过微信进行认证。 场景说明
密码认证	访客二维码认证服务器	在外来访客场景下，访客在得到内部员工的审批后才能正常访问互联网，给访客带来良好体验的同时，内部也能对外来访客进行有效的管理。
	会议室二维码认证服务器	会议室开会上网体验，或小范围上网体验私密体验，期望实现会议室或小范围内，接入网络上网，不允许无关人员随意接入。
	LDAP服务器	当企业网络中存在LDAP服务器的时候可使用该认证方式，需要在[认证服务器]页面先添加对应的LDAP服务器，并设置相关信息。
	RADIUS服务器	当企业网络中存在RADIUS服务器的时候可以使用该认证方式，需要在[认证服务器]页面先添加对应的Radius服务器，并设置相关信息。
	POP3服务器	当企业网络中存在POP3服务器的时候可以使用该认证方式内，需要在[认证服务器]页面先添加对应的POP3服务器，并设置相关信息。
	OA	当企业内部使用的OA账号为（企业微信、阿里钉钉、口袋助理等），AC均支持该

认证方式	账号认证服务器账号	类OA账号实现Oauth认证。
		场景说明 当企业内部使用社交账号（Facebook、Gmail、Line、Twitter）时，AC支持对接并实现Oauth认证。
单点登录		
	第三方认证系统CAS、OAUTH、SAML2.0	当企业内部使用CAS、OAUTH或SAML2.0认证系统时，可使用AC设备对接该系统认证。
	AD域	当企业网络中已有AD域服务器做用户管理，并且内网用户登录电脑系统都是使用域账号登录的，那么可以采用域单点登录的方式，在内网用户登录到域之后就通过设备的认证，即终端用户登录域即可上网，无需通过设备再次认证。
	PPPoE	当用户环境中存在PPPoE拨号场景时，并且PPPoE拨号认证的数据包经过AC设备时，可以启用PPPoE单点登录，认证成功后以PPPoE拨号的用户名在AC上线。
	Radius	当用户环境中存在Radius服务器，并且Radius认证和计费的数据包经过AC设备时，可以启用Radius单点登录，认证成功后以Radius的用户名在AC上线。
	Proxy	如果用户网络环境中已经部署代理服务器，并且内网用户使用代理服务器上网都有账号和密码，那么可以采用Proxy单点登录的方式，在内网用户通过代理服务器的验证之后就通过设备的认证，即终端用户连接到代理服务器即可上网，无需通过设备再次认证。
	POP3	如果用户网络环境中已经部署POP3邮件服务器，并且内网用户登录邮件服务器都有各自的账号和密码，那么可以采用POP3单点登录的方式，在内网用户通过POP3服务器的验证之后就通过设备的认证上网。
	Web	如果用户网络环境中已经部署WEB服务器，并且内网用户登录WEB服务器都有各自的账号和密码，那么可以采用WEB单点登录的方式，在内网用户通过WEB服务器的验证之后就通过设备的认证上网。

认证方式	第三方服务器认证场景说明	某些网络环境中已经存在其他的第三方认证系统做用户认证和组织结构的管理，此时设备能够跟这些第三方的认证系统结合使用，做单点登录。目前设备支持的其他第三方厂商的认证系统有锐捷Sam系统、HTTP单点登录接口、H3C CAMS系统、城市热点、H3C IMC系统和华为Agile Controller。
	深信服设备	AC设备还能够同第二台AC/SG设备结合做认证，相当于网络环境中部署了两台SANGFOR设备，其中一台设备作认证，另外一台设备作审计控制，只要用户通过了认证设备的认证后，审计控制设备就能够同步认证设备的用户信息，对用户进行审计控制。
	数据库认证	当网络环境中已有一套数据库系统存储并管理用户认证信息、组织结构的情况下，深信服 AC设备支持配置SQL查询语句，查询该数据库系统中的用户列表和已认证用户，并同步到设备的组织结构和在线用户列表中，从而支持和数据库系统结合的单点登录，实现用户通过数据库认证后，即通过设备的用户认证，同时用户从数据库认证系统中注销，也自动完成在设备上的注销。目前支持的数据库类型有ORACLE、DB2、MYSQL几种。

Portal认证

Portal认证也称Web认证，以浏览器或客户端的形式为用户提供身份认证等个性化信息服务。Portal认证包括了认证策略、认证服务器、单点登录、认证页面定制等模块，通过这几种功能的灵活搭配满足多样化的认证方式需求。

认证策略

内网的所有终端上网前，都必须经过用户认证，以识别上网计算机的身份，减低内网的安全风险。认证策略决定了某个IP/网段/MAC地址的计算机上网的认证方式。通过认证策略设置内网用户的认证范围、认证方式以及认证后处理。

6.2.1.1.1.**认证策略配置**

认证策略是从上往下逐条匹配的，可以通过页面上的移动按钮来调整认证策略优先级。通过认证策略可以为不同的网段配置不同的认证方式。

管理员可以对所有的认证策略进行删除操作、批量编辑、启用和禁用、导入、上移/下移等操作，也能进行过滤选择。

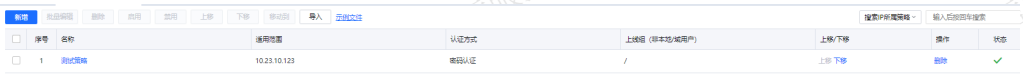


表10认证策略界面说明

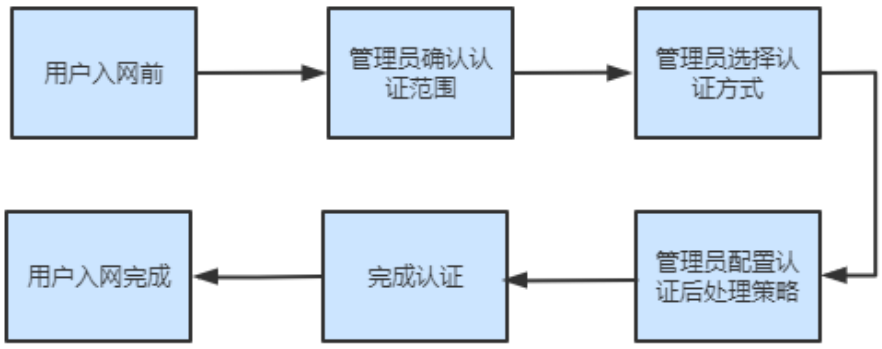
操作	功能说明
新增策略	认证策略列表页面，可点击新增一条新的认证策略。
删除策略	认证策略列表页面，可点击删除相应的策略。

编辑/批量编辑	在认证策略列表页面，勾选需要编辑的认证策略，点击认证策略名称，设备会弹出认证策略的编辑页面，修改选中策略的相关信息。 批量编辑：勾选多个自定义的认证策略，可编辑策略的适用对象，其他信息不可以修改。
导入	支持认证策略的导入，点击导入，选中需要导入的认证策略文件，即可进行导入。
启用/禁用	选中已禁用的策略，点击启用，该策略即可生效，选中已启用的策略，点击禁用，该策略会失效。
上移/下移/移动到	由于策略是自上而下进行匹配，所以可以选中相应的策略，点击上移或者下移，或自定义移动，来进行优先匹配策略。
搜索	可通过IP地址、VLAN信息、MAC地址搜索匹配的认证策略。

配置思路

1. 管理员确定需要认证的范围。
2. 选择认证方式和认证后处理策略之后完成认证，方便后续策略下发。

如下是认证策略配置流程图。



第一步：配置认证范围：

进入[接入管理/接入认证/PORTAL认证/认证策略]页面，点击<新增>，添加一条认证策略，填写策略名称和描述。

选择设备：选择该条认证策略生效的设备范围，在AC启用认证中心时使用，可选择所有或根据需求选择，默认选择所有（未启用认证中心功能时，只能选择所有）。

适用范围：设置匹配认证策略的终端和用户范围，可设置IP、IP段、MAC地址或VLAN ID，匹配到这些认证源参数的用户就使用这条策略中所设置的认证方式进行认证。

第二步：配置认证方式：

设备的认证方式如下。

表11认证方式使用说明

认证方式	使用说明
不需要认证	匹配了此种认证方式的情况下，设备会根据数据包的源IP地址、源MAC地址、上网计算机的计算机名来识别用户，不需要用户手动填充认证信息。不需要认证的识别方式，优点是用户上网前浏览器中不会弹出认证框，适用于用户上网无感知场景。
密码认证	密码认证包括本地密码认证、外部服务器认证、短信认证、微信认证、二维码认证和Oauth认证等（可同时启用多个），适用于用户需要输入用户名密码进行验证通过才能入网的场景。其中外部服务器认证为接入终端将认证信息发给AC设备，AC设备转发给第三方服务器设备，根据返回的结果来决定是否通过认证。同时，当密码认证使用本地密码认证、LDAP、Radius、POP3、短信认证、微信认证、短信快捷、微信快捷认证时，支持动态码双因素认证。
单点登录	当用户有自己的第三方认证服务器对内网用户进行认证时，单点登录可以实现在内网用户通过第三方认证服务器认证的同时通过AC设备的认证，并且获取到相关的权限上网。设备上使用和第三方认证服务器同一套用户名密码。目前设备支持的单点登录类型包括：AD域单点登录、Radius单点登录、Proxy单点登录、POP3单点登录、Web单点登录、数据库单点登录、深信服设备以及其他第三方设备单点登录（如锐捷Sam系统、HTTP单点登录接口、H3C CAMS系统、城市热点、H3C IMC系统和华为Agile Controller）。
不	

允许认证（禁止上网）	适用于禁止用户上网的场景。认证方式选择“不允许认证”时，符合IP、MAC范围的用户是不能通过AC认证上线的，此时包括单点登录用户、Dkey用户都无法认证上线，
Dkey认证	Dkey认证的优先级最高，即用户已经使用其他认证方式在AC设备上线，该用户再使用Dkey认证，则Dkey认证会顶替其他认证方式，最终以Dkey用户的身份认证上线，适用于key认证和存在特权用户的场景。

1. 不需要认证

设备会根据数据包的源IP地址、源MAC地址、上网计算机的计算机名来识别用户。可选[以IP地址作为用户名]、[以MAC地址作为用户名]、[以计算机名作为用户名]。

2. 密码认证

密码认证包括本地密码认证、外部服务器认证、短信认证、微信认证、二维码认证和Oauth认证（可同时启用多种供用户选择）。同时，当密码认证使用本地密码认证、LDAP、Radius、POP3、短信认证、微信认证、短信快捷、微信快捷认证时，支持动态码双因素认证。

涉及到具体认证服务器配置可看认证服务器章节。

3. 单点登录

当企业已有自己的第三方认证服务器对内网用户进行认证时，单点登录可以实现内网用户通过第三方认证服务器认证的同时通过AC设备的认证，并且获取到相关的权限来上网。设备和第三方认证服务器共用同一套用户名密码。

目前设备支持的单点登录类型包括：AD域单点登录、Radius单点登录、Proxy单点登录、POP3单点登录、Web单点登录、数据库单点登录、深信服设备以及其他第三方设备单点登录（如锐捷Sam系统、HTTP单点登录接口、H3C CAMS系统、城市热点、H3C IMC系统和华为Agile Controller）。涉及到具体单点登录服务器配置可看认证服务器章节。

4. 不允许认证：

认证方式选择“不允许认证”时，符合IP、MAC范围的用户是不能通过设备认证上线的，也就是禁止上网，此时包括单点登录用户、Dkey用户都无法认证上线。

5. Dkey认证：

Dkey认证的优先级最高，即用户已经使用其他认证方式在AC设备上线，该用户再使用Dkey认证，则Dkey认证会顶替其他认证方式，最终以Dkey用户的身份认证上线。需要注意的一点是：如果某些IP、MAC范围在[认证策略]中设置了不允许认证，则Dkey用户使用这些IP、MAC上网也无法认证通过。Dkey认证用户只需要在[用户管理/高级选项/Dkey用户]中直接添加用户即可，不需要单独针对Dkey用户设置一条[认证策略]。需要使用Dkey，具体配置可以参考Dkey用户。

第三步：配置认证后处理：

认证后处理是用于设置用户认证通过后，可选非本地/域用户使用该组上线、自动录入到用户到本地组织结构、自动录入绑定关系。

• 非本地/域用户使用该组上线：当非AC本地用户、非AD域用户认证后，用户使用哪个组权限上线，关联该组的上网策略。

• 自动录入用户到本地组织结构：当非AC本地用户、非AD域用户认证后，用户是否自动添加到AC的本地组织结构。如果勾选的话则匹配[非本地/域用户使用该组上线]中选择的组，将认证的用户加到对应的组中。

• 如果选择自动录入到本地组织结构，可以选择[允许多人同时使用]或[仅允许一人使用]。

• 自动录入绑定关系：用于设置用户认证后（包括本地用户、域用户和新用户），是否自动录入绑定认证后IP和MAC对应关系，是否自动录入绑定认证后的用户名和IP/MAC对应关系。具体可参考用户绑定管理章节。

• 用户使用新终端登录时需审批：当用户换了新的终端，可勾选需要审批。

高级选项：

在[高级选项]可以设置认证前使用此组权限、启用用户登录限制、免认证用户上线前弹出提示页面、此策略认证范围内不允许认证相关的操作。

• 认证前使用此组权限：认证放通或拒绝某些应用/网址，需要先配置上网策略，然后再关联此组。

• 启用用户登录限制：用户限制加强，定义认证策略黑白名单组。

• 免认证用户上线前弹出提示页面：勾选后会对免认证用户进行弹窗提醒，告知用户当前是免认证，或者是自定义的提醒内容。

• 此策略认证范围内不允许免认证：如果在其他策略配置免认证，勾选此功能项后该策略认证范围内的所有终端用户免认证都不生效，排错时候注意检查。

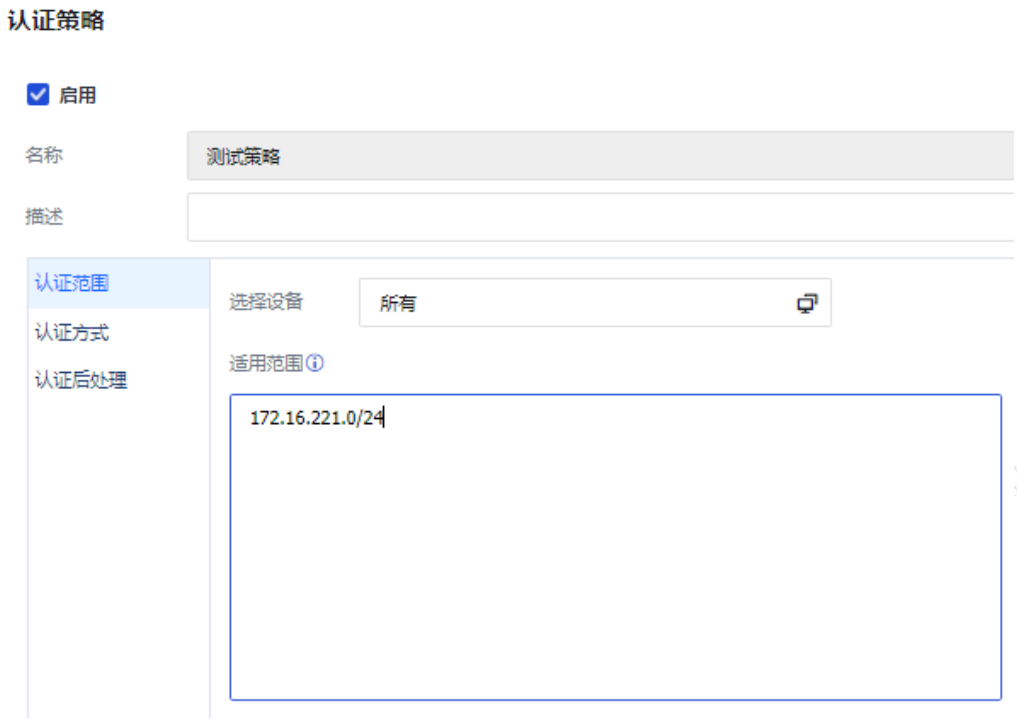
6.2.1.1.2.常用认证案例

不需要认证

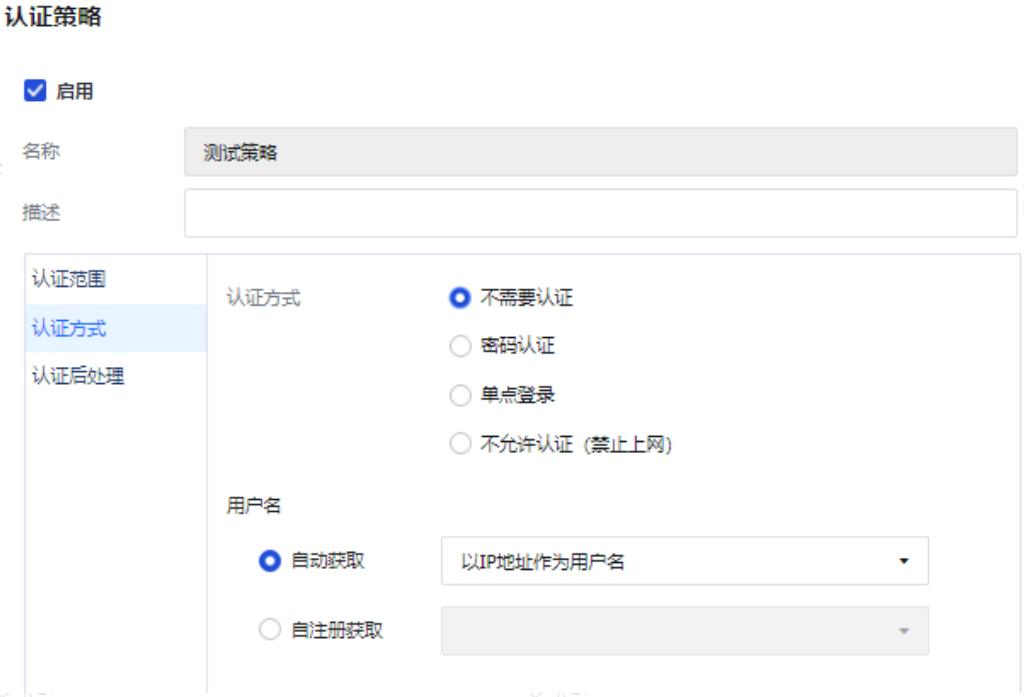
配置案例1：某企业要求内网172.16.221.0/24网段的用户上网认证的过程是透明的，不会感知AC的存在，用IP标识终端身份，使用不需要认证的方式上线，上线后用户不添加到组织结构，使用“/内部组/”的权限上网。

操作步骤

步骤1.在[接入管理/接入认证/PORTAL认证/认证策略]，点击新增认证策略进行配置，设置认证范围：172.16.221.0/24。

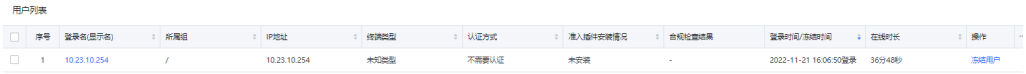


步骤2.设置认证方式：选择不需要认证，用户名：选择以IP地址作为用户名。



步骤3.设置认证后处理：该案例要求认证成功的用户不用添加的组织结构，则不勾选[自动录入用户到本地组织结构]，认证成功后使用“/内部组/”的权限上网，则在[非本地/域用户使用该组上线]中选择“/内部组/”。

步骤4.用户以IP为用户名上线，在线用户列表可以查看用户信息。



不需要认证2

某企业要求内网10.10.10.0/24网段的用户使用不需要认证的方式上网，用户认证后以IP为用户名自动添加到组织结构，添加到“/内部组/”，由于内网IP是固定分配的，客户想要通过在AC上自动绑定IP、MAC的关系，确保内网用户上网不能随便修改IP地址，一旦用户随便修改了IP，则在AC上认证不通过，无法上网。内网到AC设备有跨三层交换机。

操作步骤

步骤1.参考配置案例1的步骤1和步骤2。

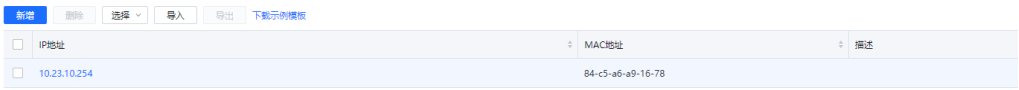
步骤2.认证后处理：该案例要求认证成功的用户添加到“/内部组/”。

步骤3.[非本地/域用户使用该组上线]：选择“/内部组/”，勾选[自动录入用户到本地组织结构]，勾选[自动录入IP和MAC的绑定关系]。设置完点击<提交>。

步骤4.因为内网到AC是跨三层的环境，AC要启用SNMP功能，通过SNMP协议获取交换机上的用户真实MAC，这种场景需要内网交换机支持SNMP功能。在[接入认证/联动对接设置/跨三层取MAC]页面，配置三层交换机的IP、MAC及SNMP信息，详细配置参考跨三层取MAC章节。

步骤5.用户上线时，是以IP用户名认证上线，如下所示。

步骤6.用户认证时的IP/MAC绑定关系自动录入，可以在[IP/MAC绑定]页面进行查询。



本地密码认证

某企业要求对内网172.16.1.0/24网段的用户使用本地密码认证方式，认证成功后自动录入本地用户，并且将用户名和IP自动绑定。

操作步骤

步骤1.首先在[接入管理/本地组/用户]添加用户，自定义登录名、密码。更多添加用户配置可参考新增用户章节。

步骤2.在[接入认证/PORTAL认证/认证策略]页面，点击<新增>，添加一条认证策略，勾选启用，用于启用这条认证策略。

步骤3.点击<新增>，添加一条认证策略，勾选启用，用于启用这条认证策略。名称：设置认证策略的名称，描述：设置认证策略的描述信息。

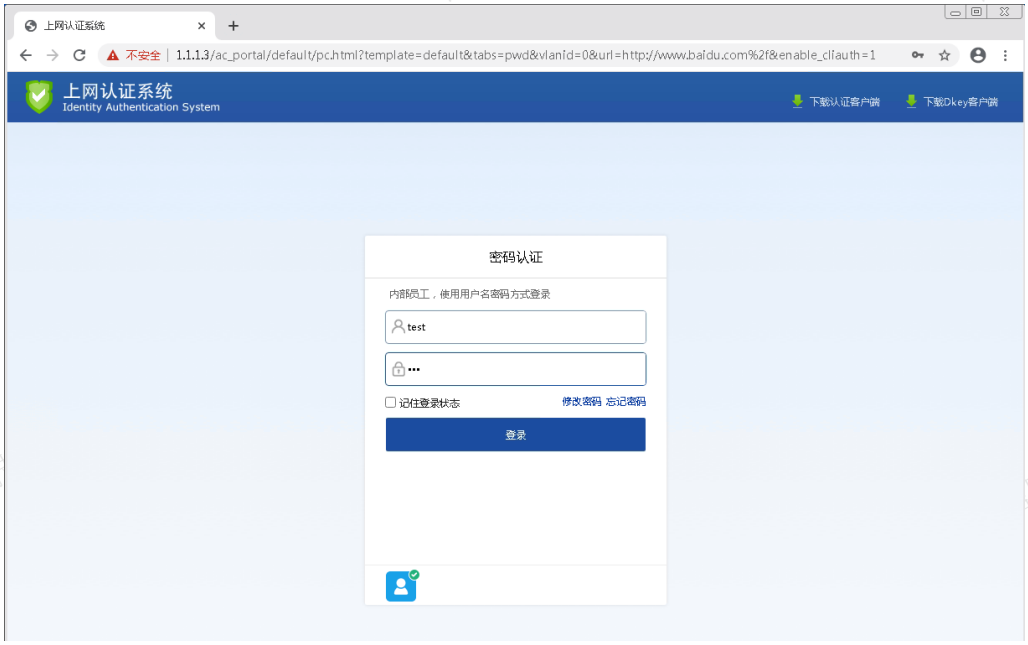
步骤4.设置认证范围：172.16.1.0/24。

步骤4.设置认证方式，选择密码认证，认证服务器选择默认的本地用户。

步骤5.点击<下一步>，配置认证后处理选中允许多人同时使用，自动录入绑定关系选中限制登录和绑定IP，有效期选中永不过期。

步骤6.认证策略设置完毕后点击<提交>，完成并保存设置。

步骤7.效果展示：用172.16.1.35这台终端去访问互联网。



步骤8.填写用户名密码后认证成功，在设备上查看用户上线，设备上查看用户名和IP的绑定信息。

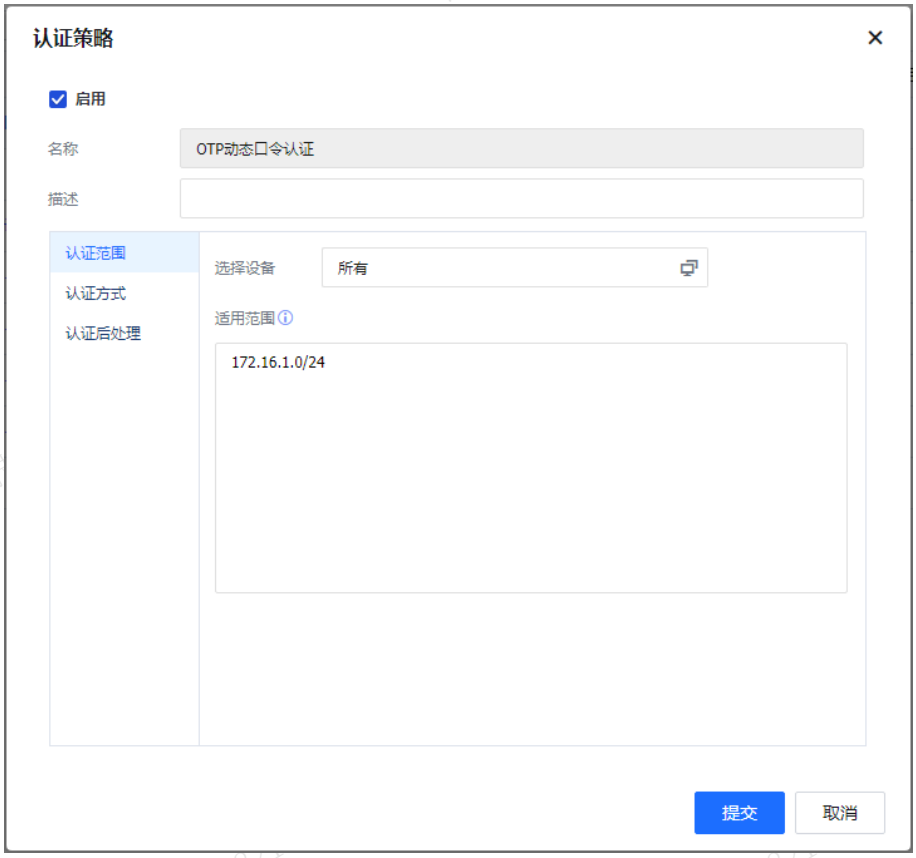
双因素认证

某企业要求对内网10.1.1.0/24网段的用户访问互联网需要通过双因素认证，首次认证采用本地密码认证，二次认证采用动态码认证。

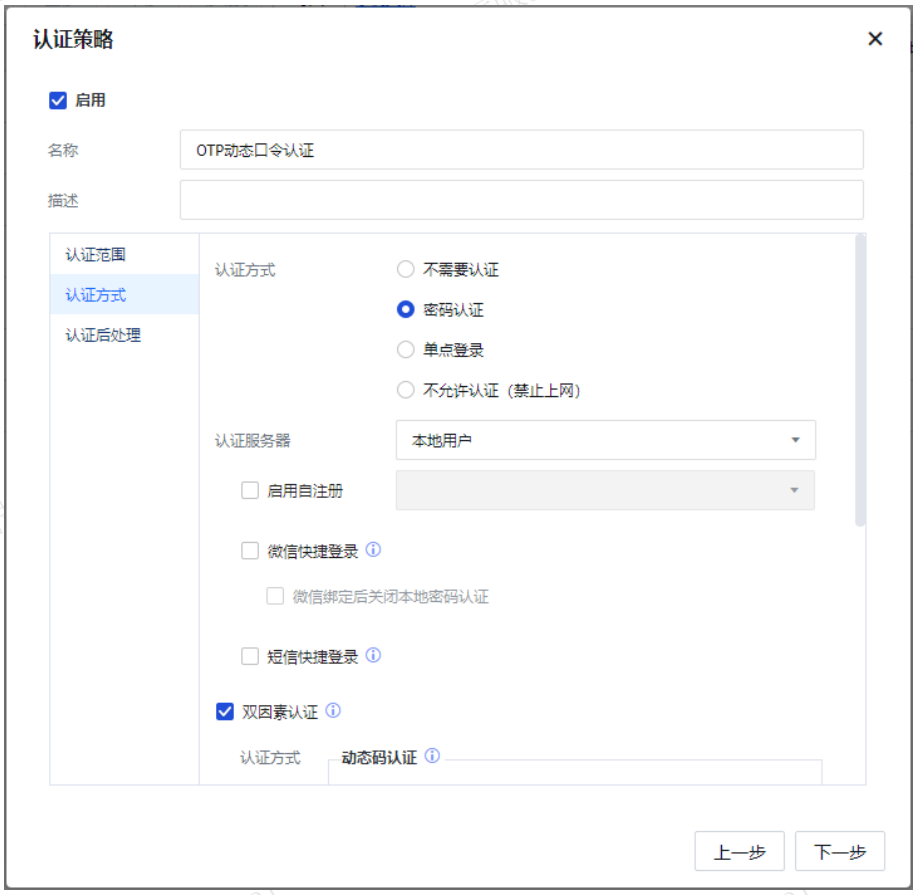
操作步骤

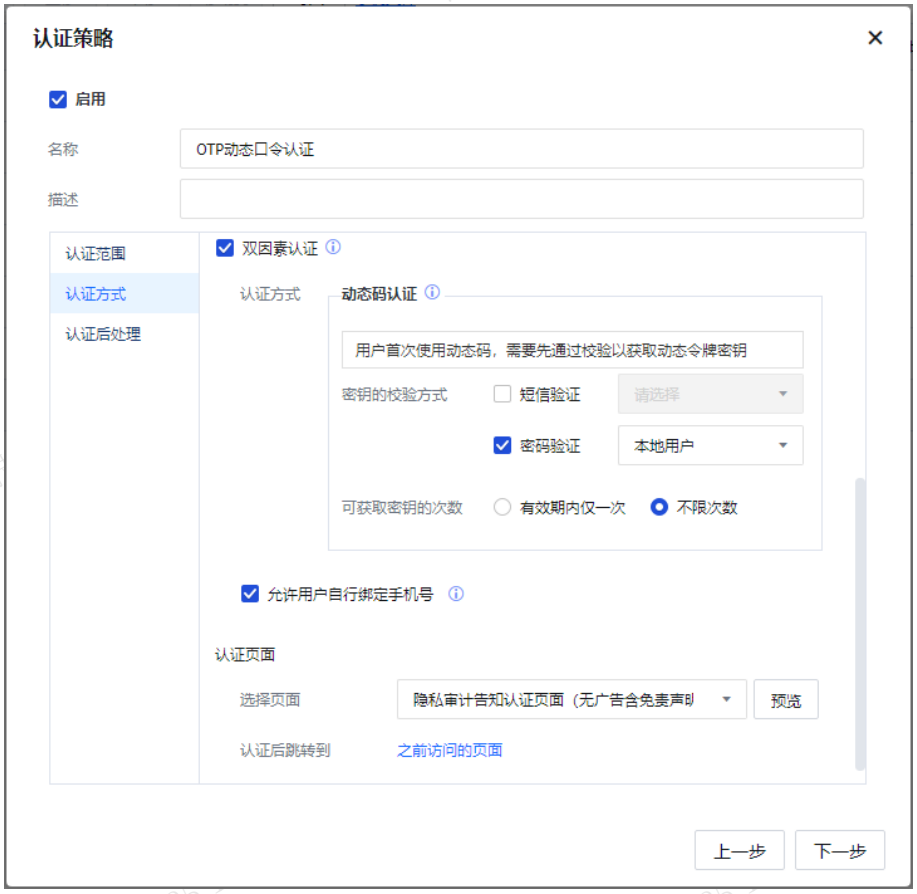
步骤1.首先在[接入管理/本地组/用户]添加用户，自定义登录名、密码。更多添加用户配置可参考新增用户章节。

步骤2.在[接入认证/PORTAL认证/认证策略]页面，点击<新增>添加认证策略，勾选<启用>，用于启用这条认证策略。填入策略名称和描述，设置认证范围：172.16.1.0/24。

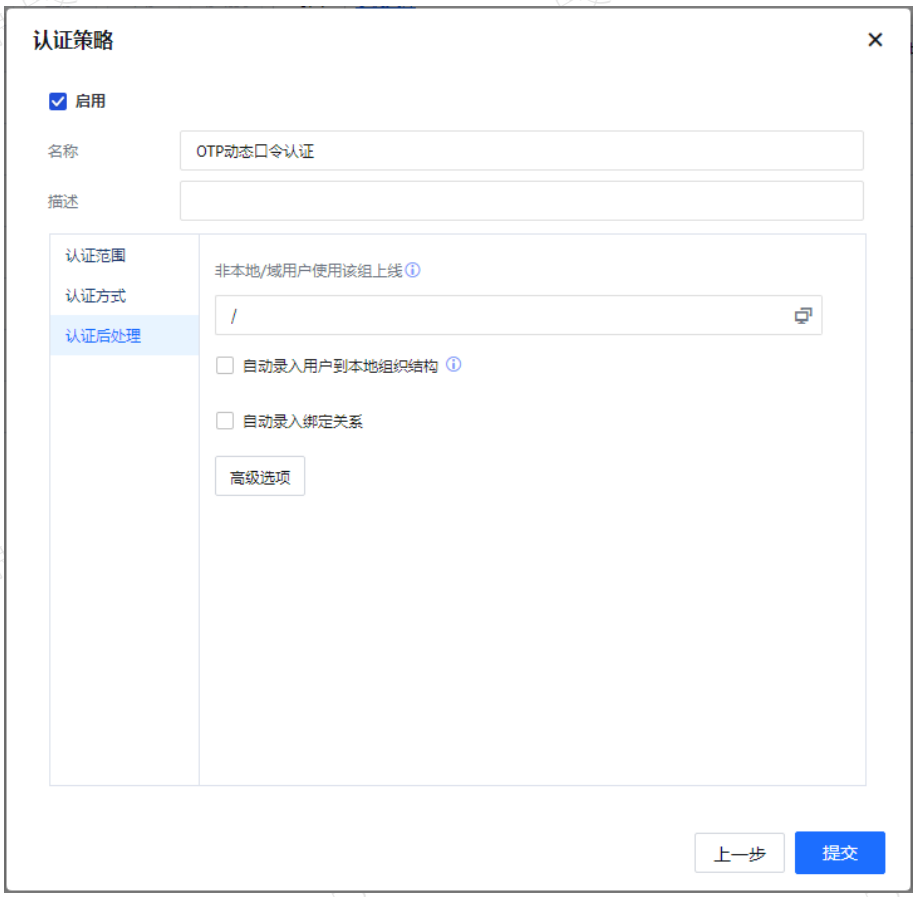


步骤3.设置认证方式，选择密码认证，认证服务器选择默认的本地用户。勾选[双因素认证]，在动态码认证中选择[密码验证]，并选择“本地用户”，可获取密钥的次数选择“不限次数”（密钥的校验方式如选择[短信认证]，需新增短信服务器）。



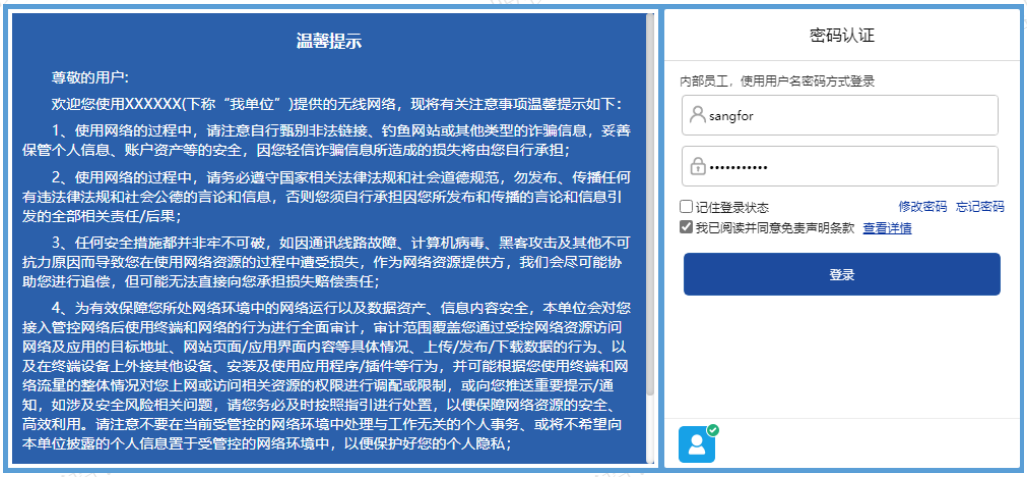


步骤4.设置认证后处理，点击<提交>完成认证策略配置

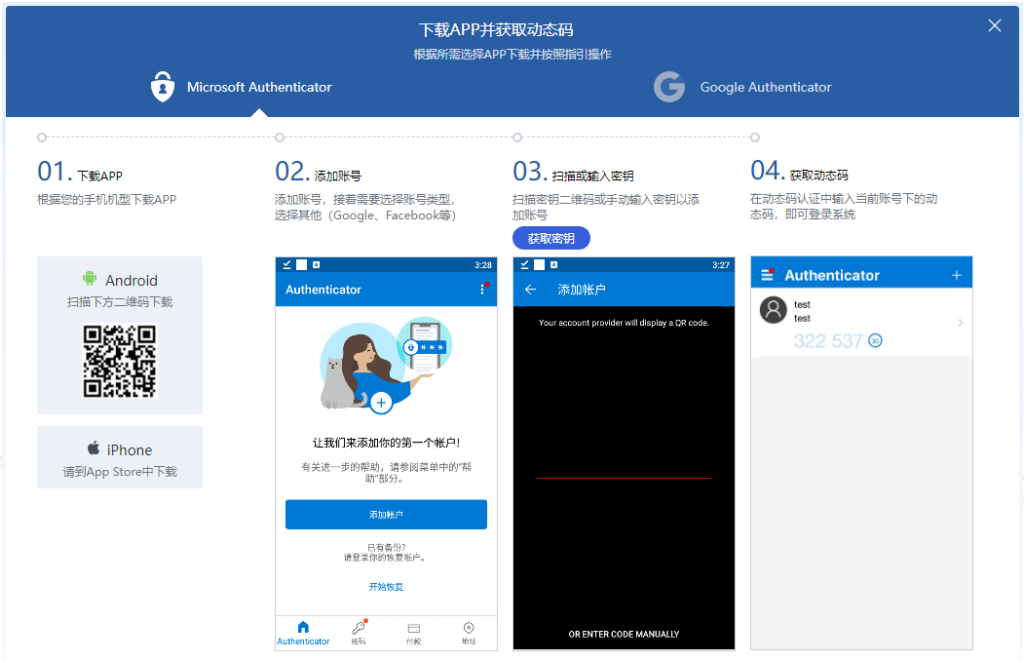


步骤5.在[接入管理/用户管理/用户绑定管理/动态令牌绑定]的高级配置中，可配置动态令牌绑定有效期（当用户动态令牌异常时，管理员可点击<重新生成>，将新的动态令牌二维码发送给用户，用于重新绑定）。

步骤6.用户打开浏览器访问互联网，重定向到认证页面，进行首次认证，输入用户名/密码，点击<登录>。



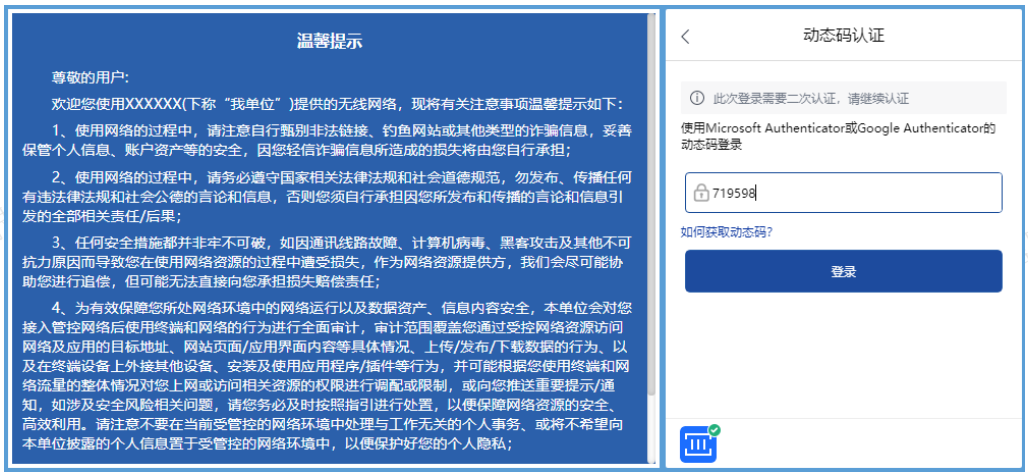
步骤7.输入用户名/密码后，跳转到二次认证页面，用户未绑定动态码时，需要先进行动态码绑定，点击<如何获取动态码？>，可查看APP下载、绑定账号、获取动态码指引。



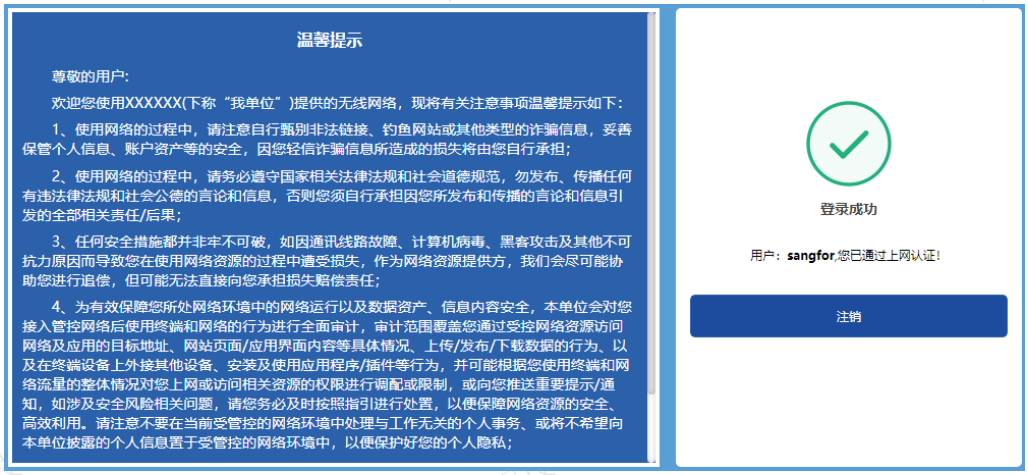
步骤8.APP可选择Microsoft/Google Authenticator任一APP，根据指引中的下载二维码或从手机应用商城中直接下载、安装。点击<获取代码>，此时需要再次进行身份验证，可选择密码认证或短信认证，认证通过后显示生成的代码二维码。

步骤9.使用已安装的Microsoft/Google Authenticator任一APP扫描代码二维码，在APP中添加账号。

步骤10.返回二次认证页面，打开Microsoft/Google Authenticator，输入动态码。



步骤11.用户完成认证。



步骤12.在AC设备中可以看到用户在线信息。

步骤13.在AC设备中可查看动态令牌已绑定。

短信快捷登录

短信快捷登录是密码认证的一种，结合短信将手机号和使用密码认证的用户账号绑定，通过获取验证码来完成认证，不需要记住密码。手机快捷登录只支持本地用户，不支持域用户。

操作步骤

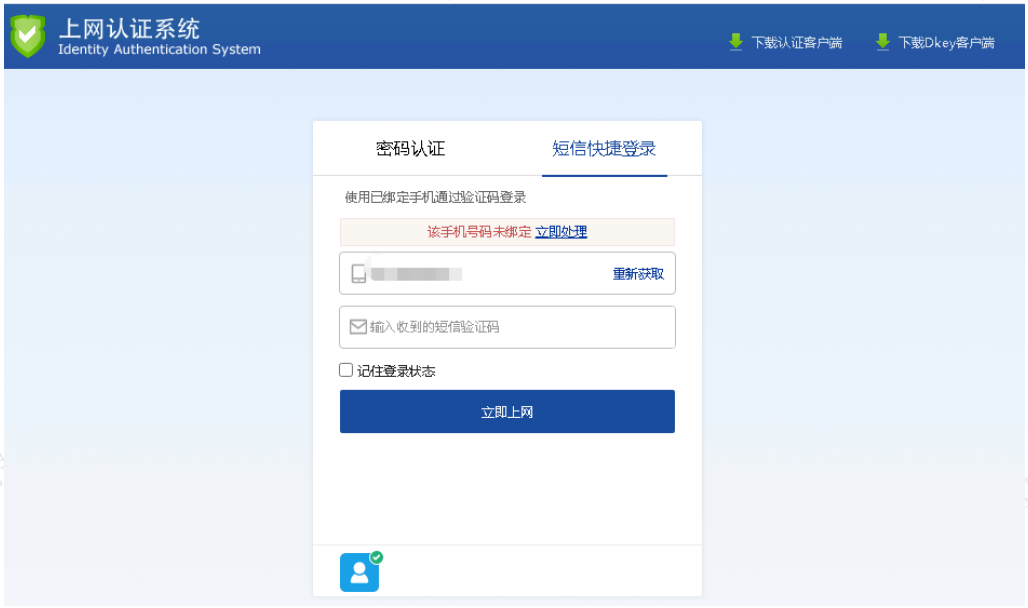
步骤1.短信通知服务器（以下以HTTP为例）和短信认证服务器参考短信认证章节。

步骤2.认证策略基本配置：管理员选择密码认证方式，设置IP段范围，认证服务器选择本地用户且勾选短信快捷登录。

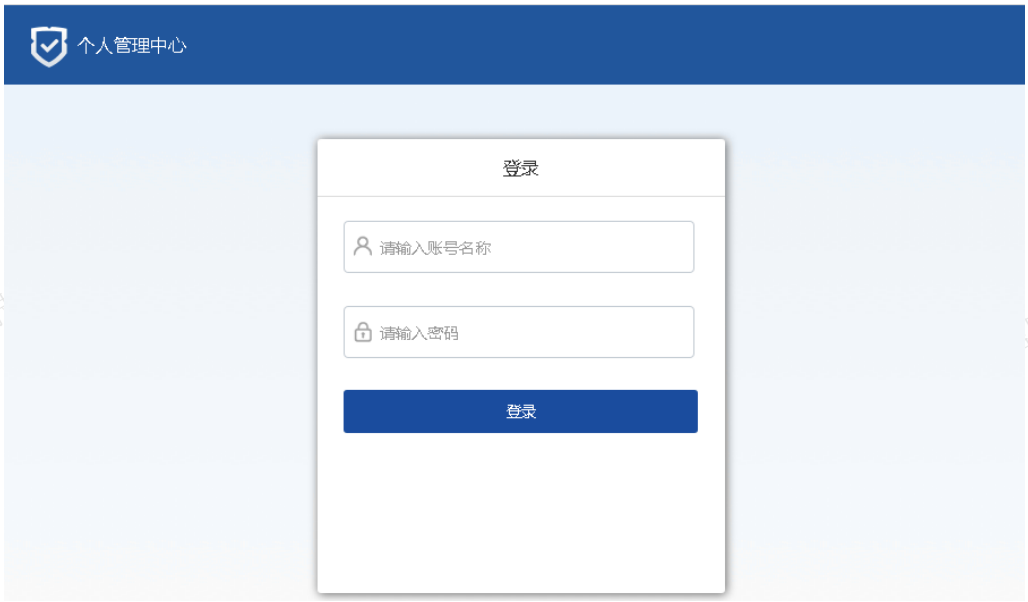
手机快捷登录&未绑定手机号&自管理录入手机号

步骤3.访问网页，重定向到认证页面。

步骤4.首次登录，发现手机号没有绑定过账号，点击“立即处理”，进行绑定。

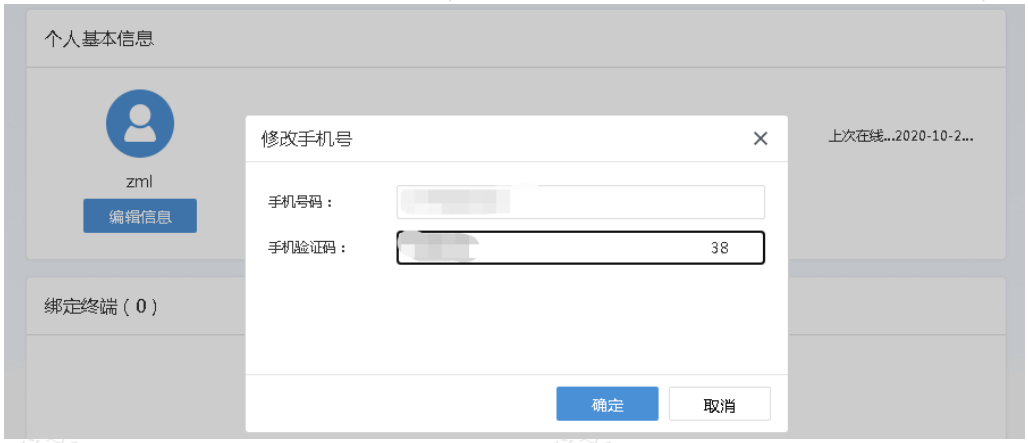


步骤5.输入用户的账号密码。

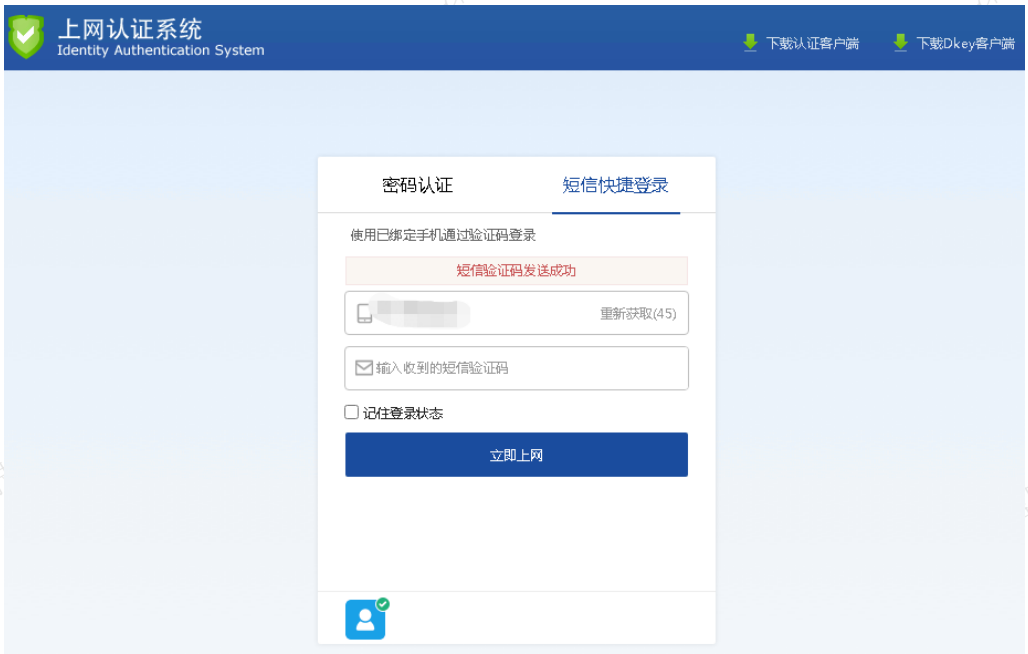


步骤6.登录后跳转到“个人管理中心”，手机字段显示“未配置”，点击进行配置。

步骤7.输入手机号和验证码进行绑定，点击确认绑定成功在个人中心会有手机信息。



步骤8.绑定完成后，重新认证，输入手机号和获取的验证码，立即上网。



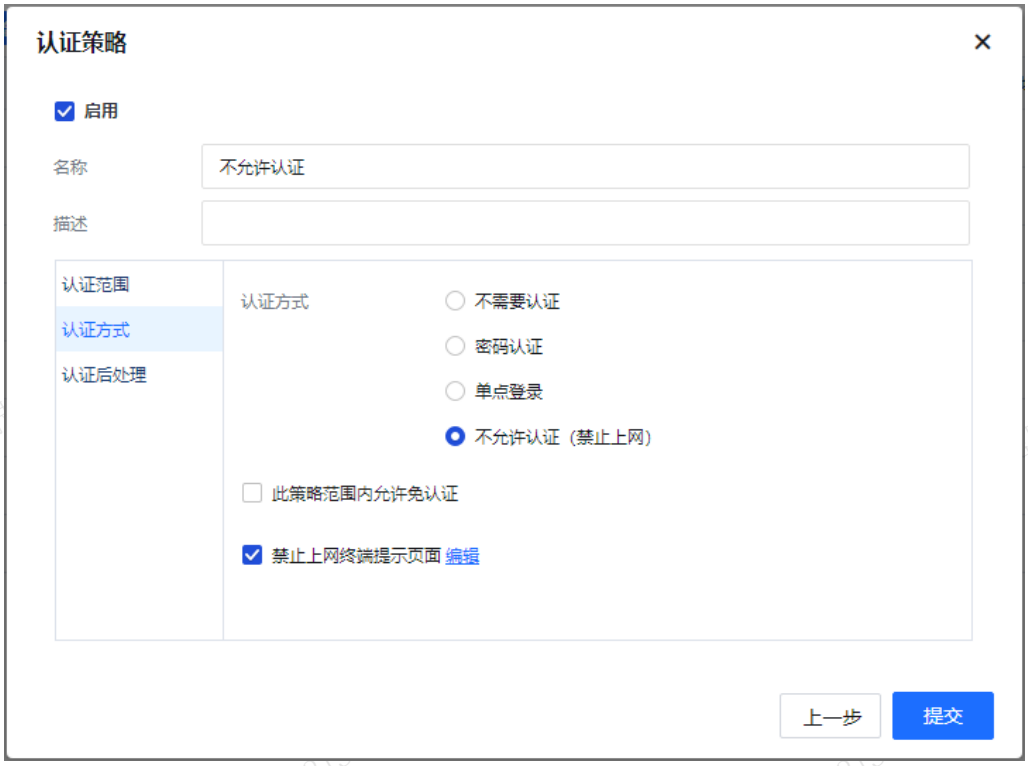
步骤9.在[全网监控/入网用户管理]可以查看用户上线成功的情况。

不允许认证

当需要让某个部门或者某个IP段的员工禁止上网的场景时，需要使用不允许认证。

步骤1.设置用户的认证策略，进入[接入管理/接入认证/PORTAL认证/认证策略]，点击新增认证策略进行配置，设置认证范围，根据需求填写不允许上网的IP或者MAC。

步骤2.设置认证方式，选择不允许认证（禁止上网），勾选禁止上网终端提示页面，禁止上网的同时，期望对用户进行告知，让用户知道当前是不允许上网的。默认情况下不勾选此功能项，请根据实际需求做选择。



步骤3.认证后处理，请根据实际需求勾选相应的功能项，点击<提交>完成配置。

步骤4.效果呈现提示用户禁止上网。

认证服务器

认证服务器用来设置第三方认证服务器的信息，设备支持定义短信、微信、访客二维码、会议室二维码、LDAP、RADIUS、POP3、OA账号、社交账号、数据库、H3C CAMS、第三方认证系统共12种认证服务器。

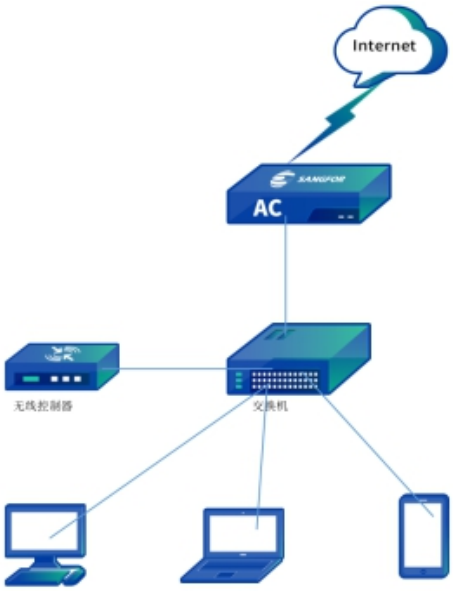
设备上使用对应的认证方式，则需要在这个页面添加对应的认证服务器，下面章节针对每种服务器做配置介绍。

6.2.1.2.1.短信认证

当使用短信认证方式时，会通过AC设备接的HTTP协议、外部服务器短信平台、短信平台、短信猫来发送验证短信给用户，用户通过输入手机收到的短信验证码认证上线。短信认证的前提是需要在外部认证服务器页面添加短信服务器，并配置正确的参数，才能认证。

使用场景

当某个单位的人员来上网需要实名制认证时，希望上网行为的日志能追溯到具体用户。可以通过短信认证的方式让访客上网前需要输入手机号和验证码验证，并将手机号作为用户名来登录上网。测试前确保AC能访问互联网。



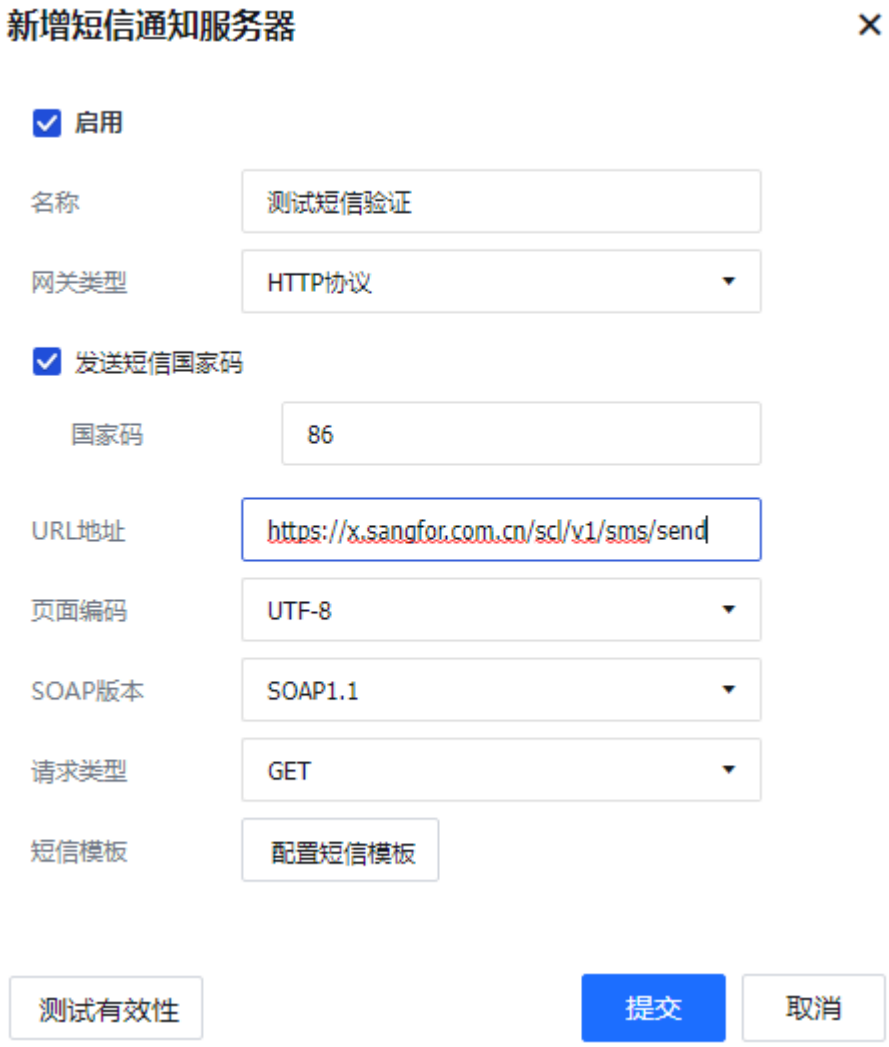
配置思路

1. 先配置短信通知服务器（以下以HTTP为例）；
2. 配置短信认证服务器；
3. 配置短信认证策略。

操作步骤

第一步：先配置短信通知服务器（以下以HTTP为例）。

步骤1.设置短信通知服务器，在[系统管理/系统配置/高级配置/通知设置]，点击<新增短信通知服务器>，勾选启用，可启用短信通知服务器。



步骤2.填写名称为：测试短信验证，网关类型：选择HTTP协议，发送短信国家码，根据需求勾选，页面编码默认即可。

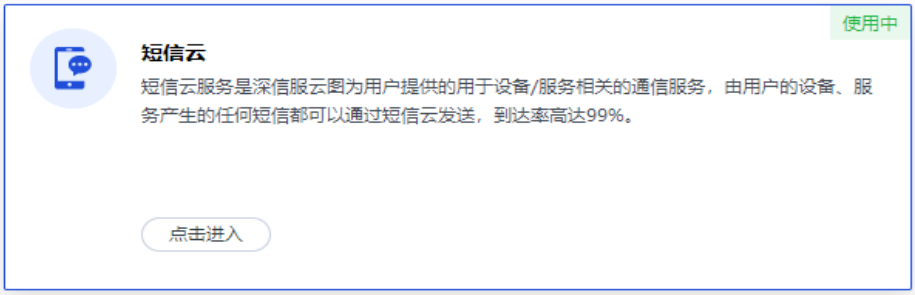
• URL地址：通过用户给予的文档，如深信服云图平台：https://x.sangfor.com.cn/scl/v1/sms/send（后续可参考短信平台提供的接口文档）。

• SOAP版本/请求类型：根据短信平台提供的接口文档（或者咨询第三方），确认使用的SOAP的版本（SOAP1.1或SOAP1.2）与请求类型（POST或GET）。

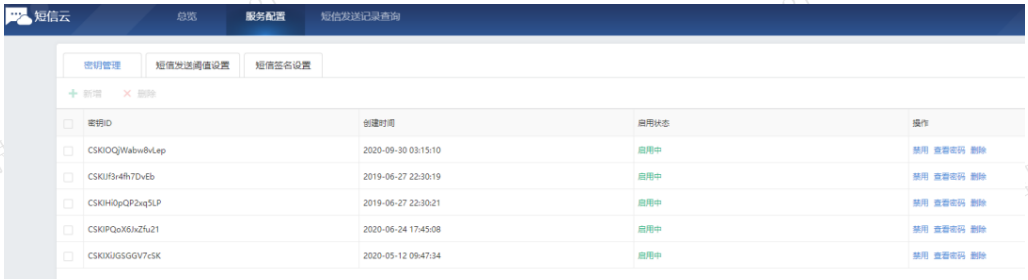
步骤3.配置短信模板，去云图平台获取参数，填写到account和password字段。接口名称和接收模板的参数，可根据自定义设置，点击<确定>配置完成。

请求模板参考：{"account":"CSKIfiKfaKemFkE9","password":"9Dww4Cfr5VtArXFrWQ5ui4BZzPhNMvIJhm","phone":"$$MOBILE_NUM$$","content":"$$SMS_CONTENT$$ "}

步骤4.对接云图平台，需先找到一台云图设备。登录设备，进入到[产品服务]章节，找到短信云。



步骤5.点击<立即进入>，跳转到短信云界面，然后点击<服务配置>章节，选择当前最新的密钥，在操作栏选择查看密码。获取到密钥ID和密码，填到短信模板的对应参数值即可。



步骤6.在[系统管理/系统配置/高级配置/通知设置]，点击<短信通知配置>，短信平台服务器选择刚配置好的“测试短信验证”策略，内容可以自定义设置或者默认，自注册审批和新终端审批通知可根据需求自定义选择即可。

步骤7.返回步骤1，点击<测试有效性>，发送一条测试短信看下能否发送成功，发送成功后，在云图短信平台的[短信发送记录查询]看到已经发送成功的手机号码的记录。

第二步：配置短信认证服务器

步骤8.在[接入管理/接入认证/PORTAL认证/认证服务器/短信认证]，点击新增<短信认证>，名称输入名称。

步骤9.短信平台选择前面配置的短信通知服务器，短信内容默认即可，根据需求是否启用“已认证用户自动绑定MAC并认证”，配置完成点击<提交>。

步骤10.短信内容：用户设定需要发送短信验证的内容。验证码有效期为10分钟。

步骤11.点击<恢复初始内容>，可以将自定义短信的内容恢复为默认值。

步骤12.已认证用户自动绑定MAC并免认证的有效期：在设置的天数内不需要重新认证。

说明：

当用户在某台终端通过短信认证成功过一次后，设备记录其登录信息，并自动绑定用户和MAC地址，在同一终端下次再接入网络时，自动通过其认证，而无需重复认证。

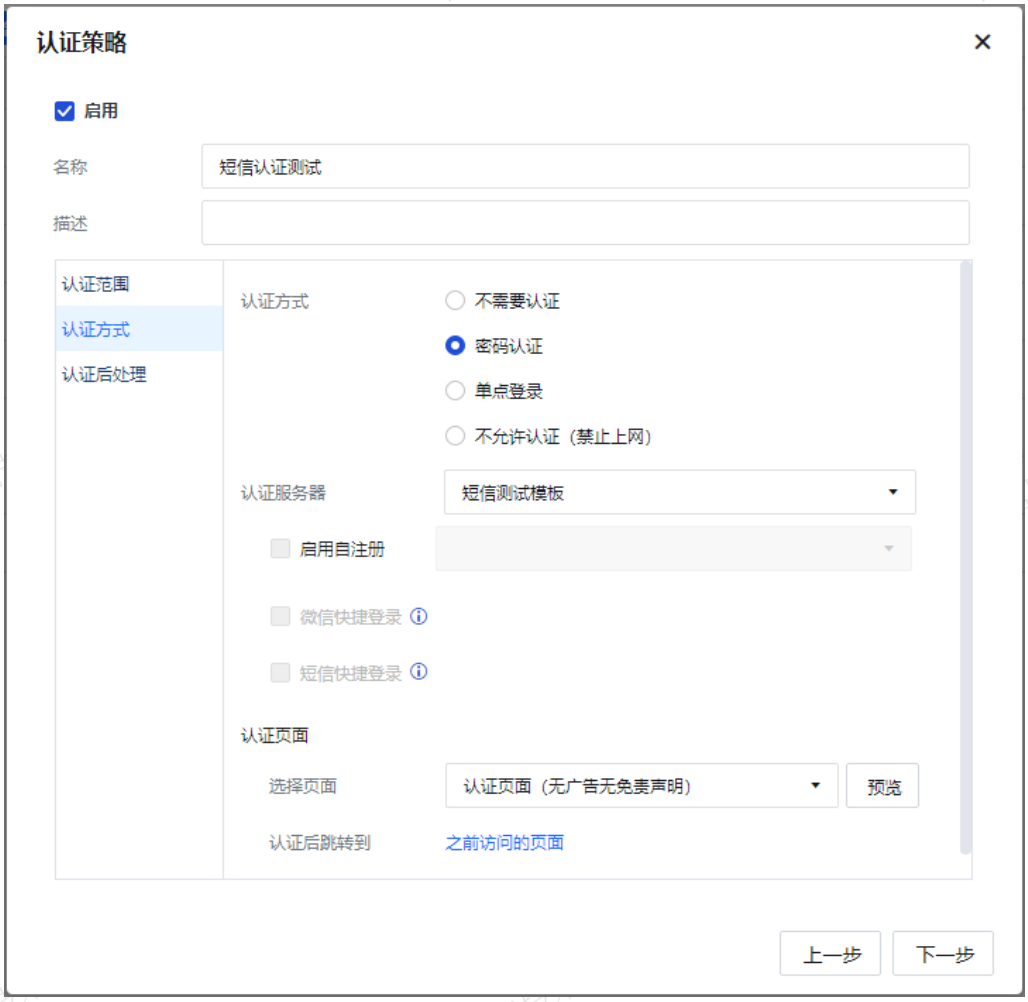
步骤13.认证过程：终端接入网络，打开网页，进行短信认证。

第三步：配置短信认证策略

步骤14.在[接入管理/接入认证/PORTAL认证/认证策略]，新增认证策略，勾选启用，填写策略名称、描述。

步骤15.设置认范围，选择设备：默认所有；适用范围：192.168.1.0/24。

步骤16.设置认证方式，认证服务器选择短信测试模板，其他选项默认即可。

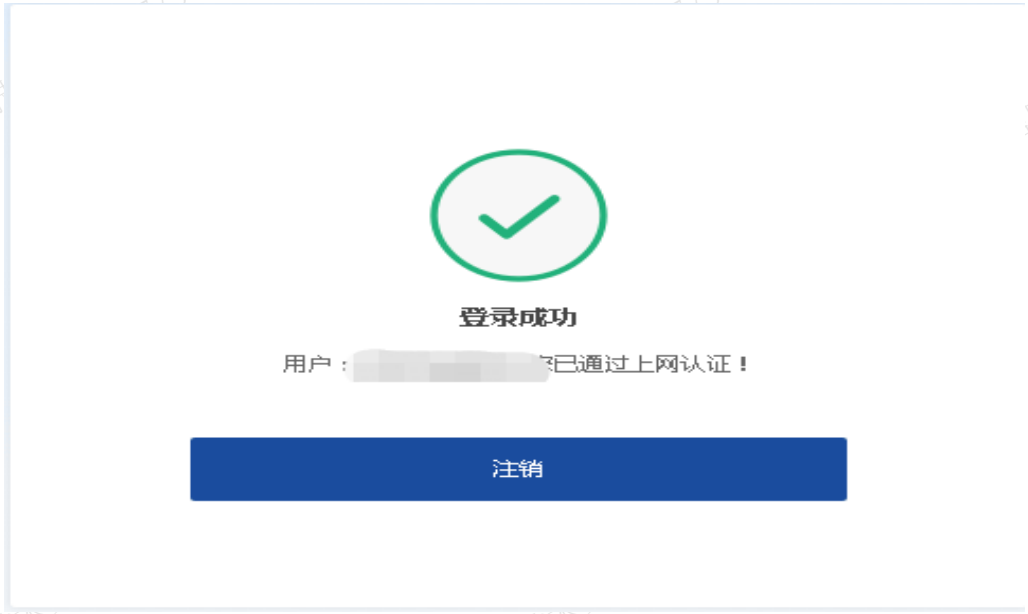


认证策略
启用
名称
短信认证测试
描述
认证范围
认证方式
认证后处理
认证方式
不需要认证
密码认证
单点登录
不允许认证（禁止上网）
认证服务器
短信测试模板
启用自注册
微信快捷登录
短信快捷登录
认证页面
选择页面
认证页面（无广告无免责声明）
预览
认证后跳转到
之前访问的页面

步骤17.设置认证后处理，选择使用“访客”组上线，其他选项默认，则短信认证成功后使用访客组的权限上网。点击<提交>完成配置。

步骤18.当终端需要上网时，会重定向认证页面。

步骤19.短信模块会向填入的手机号码发送短信验证码，手机收到验证码后，填入验证码，点击<登录>即可通过认证。



6.2.1.2.2.微信认证

当用户使用这种认证方式时，需要通过微信进行认证。微信认证的前提是需要在[认证服务器]页面，添加微信服务器，并配置正确的参数，点击<新增>，选择微信认证。

提供“下载微信认证部署说明文档及示例代码”。

• 名称：**设置微信服务器的名称。**

• 公司英文名称简称：**用于标识用户的唯唯一性，用来判断用户关注的微信公众号是否正确，填写用户英文名称或中文拼音，并以此来填写部署在第三方服务器config.php文件中的SALT字段。**

• 启用“点一点”上网方案：**这种方案的认证过程是：终端用户关注微信号后，点击[我要上网]或发送字母“W”即可通过认证。**

“点一点”上网部署方式，有以下两种部署方式：

方式一：**需要服务器部署代码**（支持服务号和订阅号）。

此种方式需要启用微信公众平台的“开发模式”，使用自身或租用的服务器部署代码响应微信的各种消息事情。具体的部署说明和代码示例在“示例代码中”可下载。

方式二：**不需要部署代码**（支持服务号和订阅号）。

配置第三方平台对接项：不需要部署Sangfor代码，从URL参数或cookie参数中提取用户的id，不做校验；此方式通常适用于微信服务商，例如微盟、微购，它们一般不能修改服务代码，但又能从URL参数或cookie中提取用户ID，就需配置第三方服务平台对接选项。具体的配置方法，提供“<与第三方服务平台对接-开发者文档>”下载。

启用“微信连wi-fi”上网方案：2019年08月19日起，“公众号连Wi-Fi”暂停微信Portal鉴权连网方式，不再提供wifi关联公众号的功能配置后台及接口，回收第三方平台微信连Wi-Fi权限集。微信官方通知：微信连Wi-Fi功能调整通知，本手册不再赘述。

6.2.1.2.3.访客二维码认证

访客二维码认证在外来访客场景下，访客在得到内部员工的审批后才能正常访问互联网，给访客带来良好体验的同时，内部也能对外来访客进行有效的管理，推荐采用访客二维码认证方式，让内部员工对每位访客的二维码进行扫码，从而满足该场景。

适用场景

• 访客填写信息，担保人扫码：**需要采集访客的信息，担保人扫码后看到访客的信息属实后，批准上网。**

• 担保人扫码，访客直接以担保人身份上线：**无采集客人信息的需求，但是想赋予访客担保人的权限，选择这种方式。**

• 担保人扫码，并备注访客信息：**不需要访客做其他操作，信息填写由内部员工完成，并在在线用户可以看到具体的担保人的信息，选择这种方式。**

操作步骤

步骤1.在[接入管理/接入认证/PORTAL认证/单点登录/认证服务器]，点击新增[访客二维码认证]服务器，勾选启用，填写名称。

步骤2.选择担保人：担保人指的是有审核权限的用户或组，如果选择的是组，则该组下所有用户都有审核权限。

步骤3.在[接入管理/接入认证/PORTAL认证/认证策略]，新增认证策略，勾选启用，填写策略名称、描述。

步骤4.设置认证范围：访客网段：192.168.10.1-192.168.10.254。

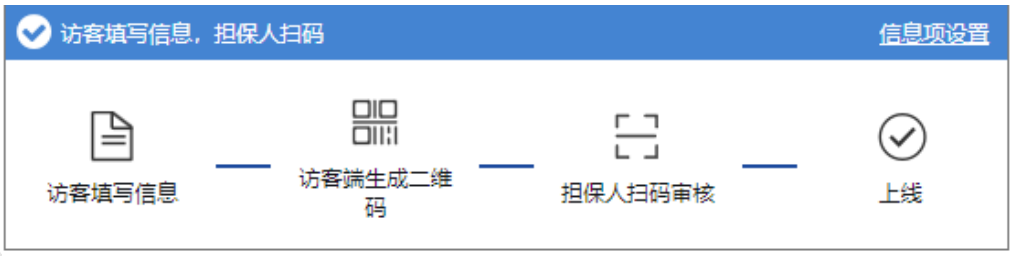
步骤5.设置认证方式，选择密码认证，认证服务器选择访客二维码。

步骤6.认证后处理，选择认证上线的组，点击<提交>即可。

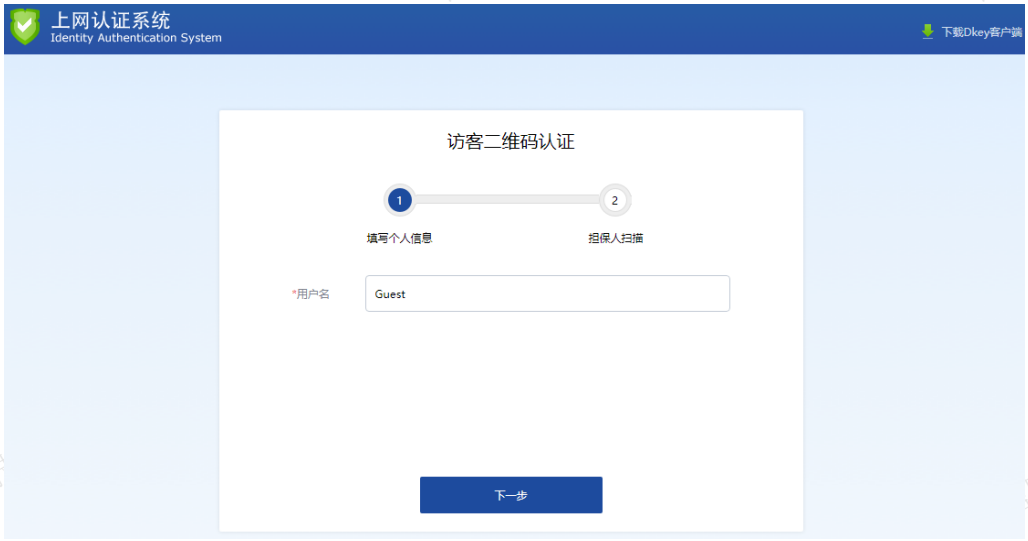
认证后效果：

访客填写信息，担保人扫码

1. 选择此认证方案：访客电脑或移动终端使用浏览器访问网页，访客填写信息—生成二维码—担保人扫码审核—审核允许后客户端通过认证并上线。



2. 在二维码认证页面填写个人信息，点击<下一步>。



3. 客户端生成二维码。

4. 内部已经上线成功的担保人用手机扫描二维码，看到访客信息，进行审核。

5. 审核通过后。

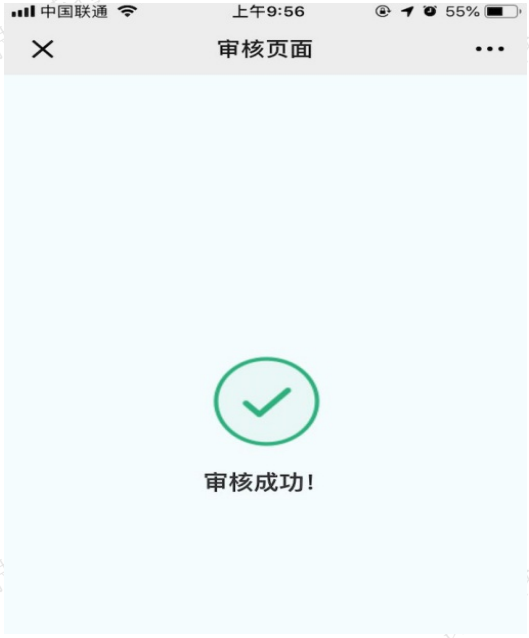
6. 访客终端，返回认证成功。完成认证，可以访问网络，设备在线用户管理，看到上线用户信息。

担保人扫码，访客直接以担保人身份上线

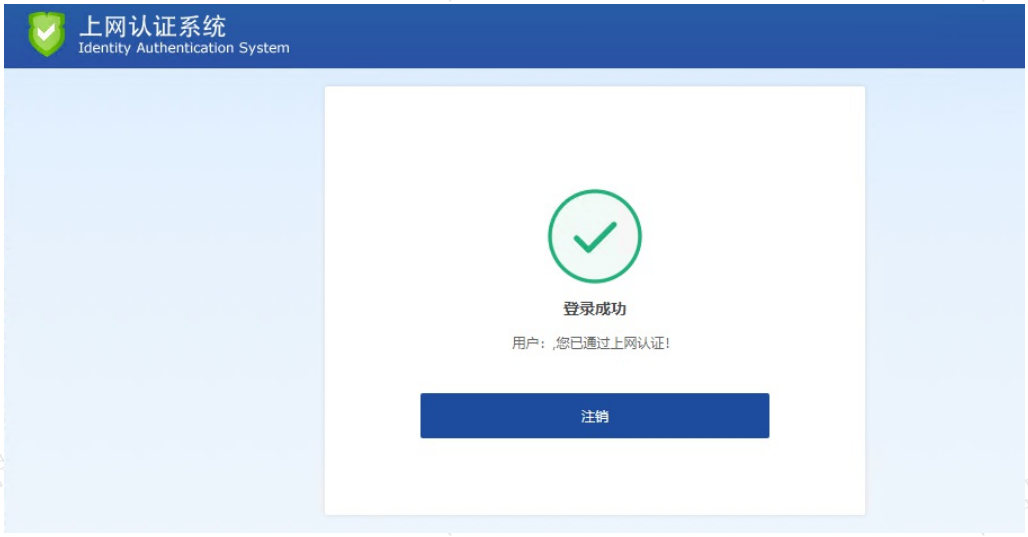
7. 选择此认证方案：访客电脑或移动终端使用浏览器访问网页，重定向到二维码认证页面，直接生成二维码，内部担保人扫描审核，完成认证。

8. 访问网页生成二维码。

9. 内部已经上线成功的担保人用手机扫描二维码。



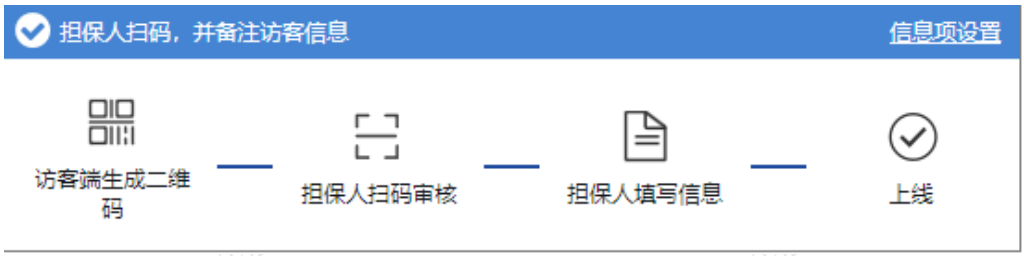
10. 访客完成认证，可以访问网络。



11. 设备在线用户管理，看到上线用户信息，但这种方式是无信息项填写的，所以无法获取到用户名，以IP地址做用户名上线。

担保人扫码，并备注访客信息

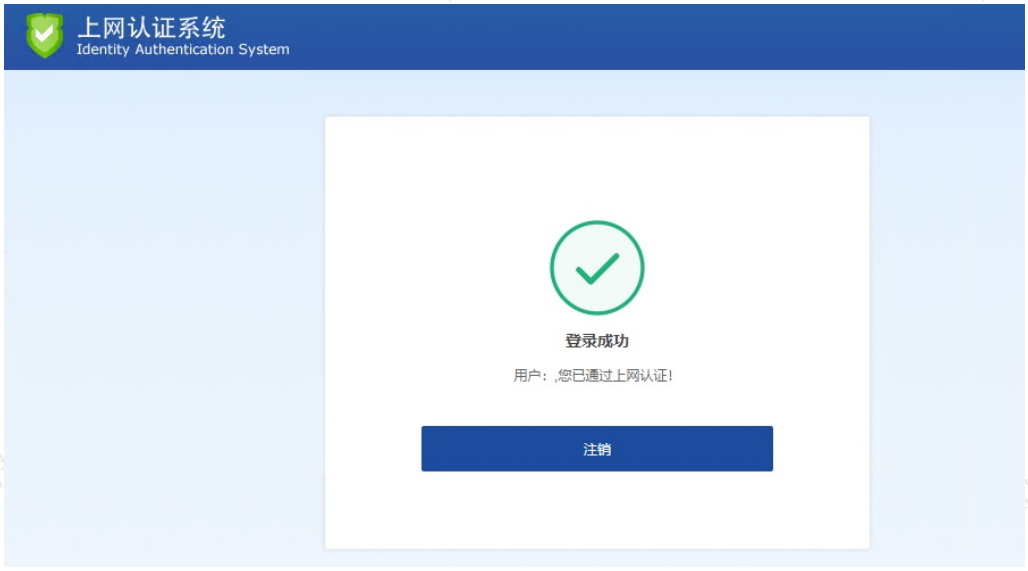
12. 选择此认证方案：访客电脑或移动终端使用浏览器访问网页，重定向到二维码认证页面，内部担保人扫描二维码填写信息，提交完成认证。



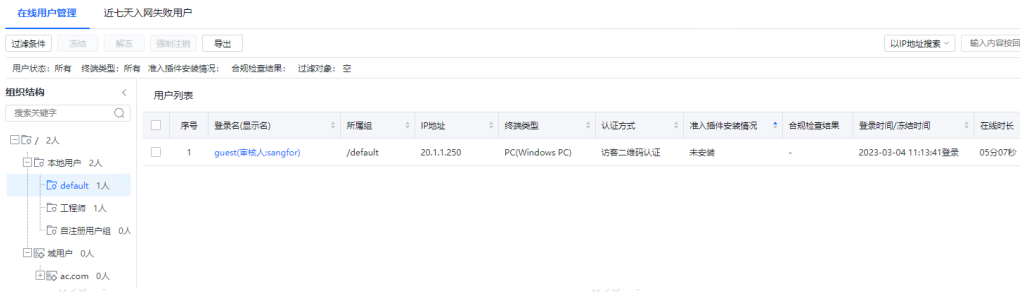
13. 访问网页生成二维码。

14. 内部已经上线成功的担保人用手机扫描二维码，在审核页面填写个人信息，点击<确定>，完成认证。

15. 访客访客完成认证，可以访问网络



16. 设备在线用户管理，看到上线用户信息，这种方式可以看到审核人的信息。



信息项设置

17. 信息项设置可以看到有两种认证方式，右上角有信息项设置，这个地方的作用是，管理员提前设置要求访客填写的信息。

18. 鼠标放置在“信息项设置”处，点击跳转到信息项设置。

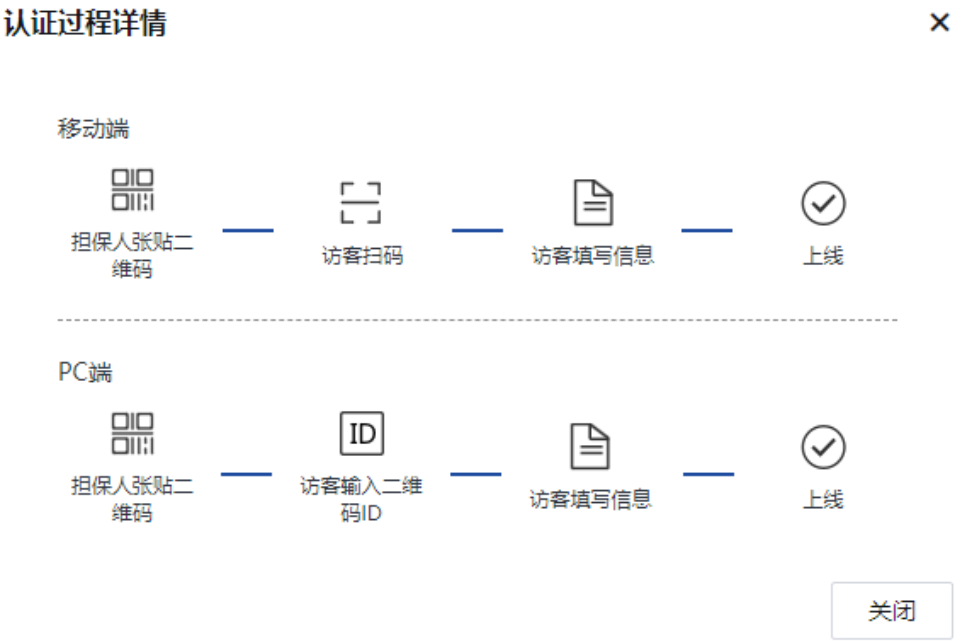
19. 进行新增访客填写的配置项：内容项是预设的，点击<新增>会跳转到[认证高级选项/自定义属性]，进行新增即可。

4. 会议室二维码认证

会议室二维码认证可实现对于会议室开会上网体验，小范围上网体验或私密体验。当用户接入网络上网，不希望被外人获知上网方法，推出了会议室二维码认证方式，实现需求。支持实名认证场景和不实名认证场景。

实现过程大致如下：

1. 用户端提供“二维码ID”（通过手动填写/扫码识别）。
2. AC设备通过二维码ID查找服务器，读取服务器的配置，返回信息项让用户填写。
3. 用户端填写信息项，提交，上线。



4. 会议室二维码认证服务器配置页面。

- 名称：**设置会议室二维码服务器的名称。**
- 用户上线组：**通过会议室二维码认证后用户上线到具体的组。**
- 二维码设置：**会议室二维码是可以张贴在会议室的，因此需要进行配置。**
- 二维码名称：**给会议室二维码取一个名字；“二维码ID”：设置一个ID，便于不能扫描的PC端输入ID接入网络；**
- 最大上线人数：**会议室或小范围的人数是有限的，对人数进行限制可以有效的管理；**
- 有效期：**二维码有效期可以定义为“永不过期”或“指定过期时间”；**
- 开启手机号实名认证：**会议室二维码如果有实名制的需求，结合手机号做实名认证。**

⚠ 注意 ：

开启手机号实名认证功能需要在[系统管理/系统配置/高级配置/通知设置]的短信通知服务器。

不实名认证场景

第一步：配置会议室二维码认证服务器

步骤1.在[接入管理/接入认证/PORTAL认证/单点登录/认证服务器]，点击新增<会议室二维码认证>服务器，勾选启用，填写会议室名称。

步骤2.二维码设置，根据需求设置二维码名称、二维码ID、最大上线人数、有效期等信息，可选择是否开启手机号实名认证。访客信息项设置可根据需求设置用户名或者其他信息都可以。

步骤3.完成配置后，点击提交就会生成二维码，或点击<会议室二维码管理>，找到对应项下载，且打印粘贴到会议室的位置。后续维护也在会议室二维码管理中。

第二步：配置会议室二维码认证策略

步骤4.在[接入管理/接入认证/PORTAL认证/认证策略]，新增认证策略，勾选启用，填写策略名称、描述。

步骤5.设置认证范围，选择设备：默认所有，适用范围：192.168.25.0/24。

步骤6.设置认证方式，认证服务器选择会议室二维码，其他选项默认即可。

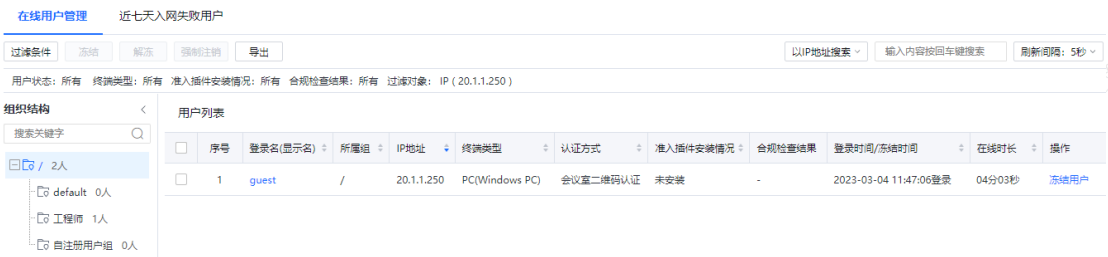
步骤7.认证后处理，默认即可，点击<提交>完成配置。

步骤8.终端通过AC上网，会重定向认证页面。

步骤9.移动端和PC端效果展示。

5. 移动端：手机扫描会议室张贴的二维码，输入信息项，点击<确定>提交。

6. 完成认证，在设备上线。

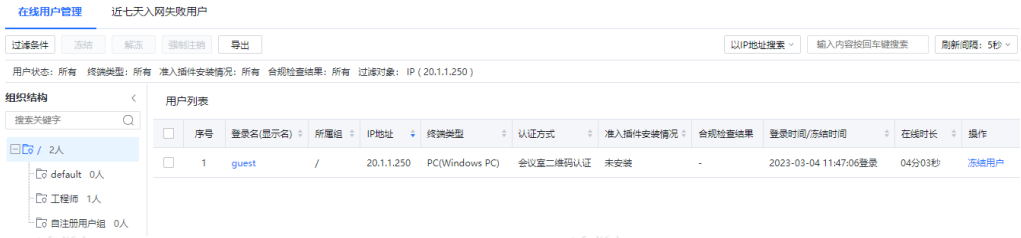


7. PC端：浏览器访问网页，跳转到认证页面。

8. 输入会议ID：1。

9. 输入个人信息完成认证，跳转到认证前访问页面。

10. 设备在线用户列表看到用户上线。



实名认证场景

第一步：配置会议室二维码认证服务器

步骤1.在[接入管理/接入认证/PORTAL认证/单点登录/认证服务器]点击新增<会议室二维码认证>服务器。

步骤2.勾选“开启手机号实名认证”后，强制手机号做用户名，完成配置后：生成二维码，可以下载打印粘贴在会议室

步骤3.完成配置后，点击<提交>就会生成二维码，或点击<会议室二维码管理>，找到对应项下载，且打印粘贴到会议室等位置。后续维护也在会议室二维码管理页面进行。

第二步：配置二维码认证策略

步骤4.在[接入管理/接入认证/PORTAL认证/认证策略]，新增认证策略，勾选启用，填写策略名称、描述。

步骤5.设置认证范围，选择设备：默认所有，适用范围：192.168.10.0/24。

步骤6.设置认证方式，认证服务器选择会议室二维码，其他选项默认即可。

第三步：短信通知服务器配置

此场景需要配合短信通知，进行实名制验证，需要先配置[系统管理/高级配置/通知设置/短信通知服务器]，确保用户可以收到短信验证码。

第四步：移动端和PC端效果展示。

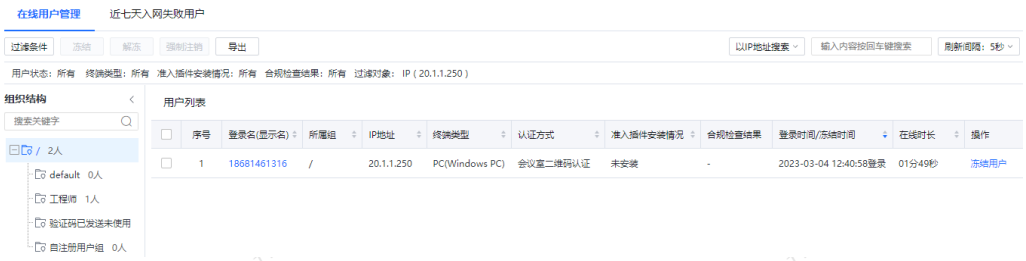
11. 移动端：手机扫描粘贴在会议室的二维码，输入手机号和信息，完成认证。

12. 设备在线用户列表看到用户以手机号上线。

13. PC端：访问网页，重定向到认证页面，输入ID。

14. 输入手机号和验证码等相关信息点击<提交>，完成认证，跳转到认证前访问页面。

15. 设备在线用户列表看到用户以手机号上线。



6.2.1.2.5.LDAP服务器

场景案例

在客户内网已经部署了LDAP服务器的情况下再部署AC，管理员希望内网用户能够使用现有的LDAP账号密码通过AC的身份认证策略，无须为内网用户在AC上再创建一套账号，从而避免用户在原有LDAP账号的基础上再记忆一套新账号和密码。

配置步骤

本次以Microsoft Active Directory作为外部LDAP服务器示例。

步骤1.在AC上配置外部认证服务器。在[接入管理/接入认证/PORTAL认证/认证服务器]界面配置外部认证服务器，点击<新增>按钮选择[LDAP服务器]。

步骤2.配置LDAP服务器相关参数。在[服务器名称]栏定义外部认证服务器的名称，在服务器类型：选择MS Active Directory(视实际情况选择对应的类型)。

• IP地址：填写LDAP服务器的IP地址。

• 认证端口：LDAP服务器连接的端口。例如AD域在未启用SSL/TLS加密时默认端口为389。

• 超时：设定认证请求的超时时间。当AC把认证请求转发到LDAP服务器后，如果超过这个时间无回应，则视为认证失败，如果AC到LDAP服务器间的网络比较慢，可尝试把超时时间延长（例如10秒）。

• 匿名搜索：如果LDAP服务器支持匿名搜索时，则可以使用此选项。

• 管理员账号：AC将使用该账号到LDAP服务器去查询以及同步的内网的用户账号。

以MS Active Directory为例：账号为administrator域名为：damian.com，那么填写administrator@damian.com。该账号拥有查询及同步AD域账号的权限（Domain Admin），并非一定要administrator账号。

• 管理员密码：管理员账号对应的密码。

• 开启加密：当LDAP服务器启用SSL/TLS加密后AC对接时也需要开启加密。且开启加密后认证端口需要更改。AD域使用SSL加密时默认为636。

• 校验证书：校验证书的合法性。如果LDAP服务器需要校验证书，请配置域名且AC能够访问到该域名。（在[系统管理/网络配置/高级设置/Hosts]里填写该域名解析到的IP）

• BaseDN：指定域搜索路径的起点，该起点决定了该条LDAP规则的生效范围。如果用户在指定的BaseDN以外，则该用户无法做外部服务器认证，所配置的策略对该用户也不会生效。所以可以通过BaseDN来划分不同管理员的所属区域。

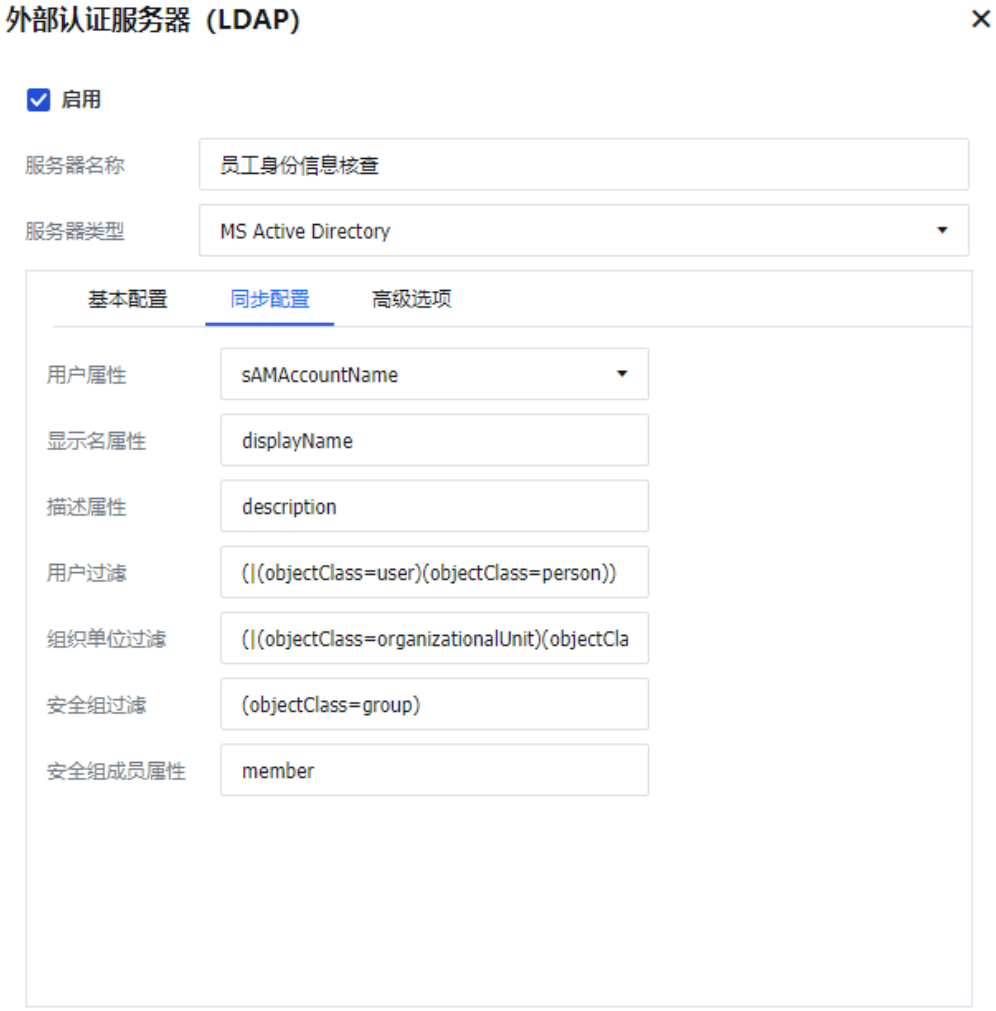
步骤3.测试连通性。点击<测试有效性>后可以测试以当前的配置对接LDAP服务器是否成功。

• 修改密码：以AD域为例：如果在AD域上创建域账号时选择了“初次登录修改密码”，那么可以直接在这里修改密码。

• 账户有效性：测试AC设备与LDAP服务器通信是否正常，校验LDAP用户账号是否有效。

步骤4.测试类型相关信息填写后，点击<测试有效性>即可验证当前配置是否有效。

步骤5.编辑同步配置和高级选项。（如果无特殊需求请保持默认值）



• 用户属性：**指定LDAP服务器上，唯一标识用户的属性字段。例如AD域上sAMAccountName属性标识了用户，而在Novell LDAP上uid属性标识了用户。**

• 显示名属性：**指定LDAP服务器上，唯一标识用户显示名的属性字段。例如AD域上displayName属性标识了用户的显示名。**

• 描述属性：**指定LDAP服务器上，唯一标识用户描述的属性字段。例如AD域上description属性标识了用户的描述。**

• 用户过滤：**指定LDAP服务器的用户过滤条件，即通过这条件可以确定某个节点是否为用户。例如AD域上可以通过填写“(|(objectClass=user)(objectClass=person))”来过滤某个节点是否为用户。**

• 组织单位过滤：**指定LDAP服务器的组织单位过滤条件，即通过这条件可以确定某个节点是否为组织单位。**

• **例如AD域上可以通过填写(|(objectClass=organizationalUnit)(objectClass=organization)(objectClass=domain)(objectClass=domainDNS)(objectClass=container))来过滤某个节点是否为组织单位。**

• 安全组过滤：**指定LDAP服务器的（安全）组过滤条件（注：对于AD域而言，这里是安全组，对于非AD域而言，这里是group），即通过这条件可以确定某个节点是否为（安全）组，例如AD域上可以通过填写“(objectClass=group)”来过滤某个节点是否为安全组。**

• 安全组成员属性：**指定AD域服务器上哪个属性标识了安全组的成员列表，该属性只有LDAP服务器为AD域的时候生效。该字段如没有特别情况，一般填写member即可。**

步骤6.当服务器类型选择“MS Active Directory”时上面这些参数是设置好的，一般采用默认参数即可，如果服务器是其他类型的LDAP，则需要根据实际情况调整，以便设备能读取到LDAP上正确的信息。

• 启用安全组实时更新：勾选该功能后AC将实时请求LDAP服务器，将所需同步的内容同步到本地，会对LDAP服务器性能增加压力。本选项只对AD域生效。

• 设置安全组和用户的关联方式：此处建议使用默认配置。

• 关联方法：可以选择“用户找组（推荐）”或“组找用户”。如果LDAP服务器上，用户存在某个属性保存了其所属组，这时可以选择"用户找组（推荐）"，因为这种方式将会提供更好的性能，同时减少LDAP服务器的性能压力。如果LDAP服务器上，用户和组之间没有相互保存的信息，只有组保存了所属用户，这种情况需要勾选“组找用户”。

• 关联属性：如果选择了“用户找组（推荐）”模式，该字段需要填写LDAP服务器上组或者用户保存其父组的属性。例如AD域上memberOf属性标识了某个节点的父组，所以搜索的时候，将使用memberOf属性来搜索其父组。如果选择了“组找用户”，该字段需要填写LDAP服务器上组保存子用户的属性。例如AD域上member属性标识了某个组的子用户，所以搜索的时候，将使用member属性来搜索某个组的子用户。

• 支持安全组嵌套：该复选框决定了配置（安全）组的时候，是对该组下的用户生效，还是对该组下的用户以及子组都递归生效。勾选该字段以后表示对应（安全）组的用户以及子组都递归生效；如果不勾选，则表示仅对配置的（安全）组下直属用户生效，忽略所有子组。

• 嵌套属性：嵌套属性只有在勾选了“支持安全组嵌套”以后才可以填写。该选项表示递归查找的时候需要搜索的组使用哪个属性来标识。如果选择了“用户找组（推荐）”模式，该字段只需要和“关联属性”保持一致即可。如果选择了“组找用户”，该字段需要填写LDAP服务器上组保存子组的属性。例如AD域上member属性标识了某个组的所有子组，所以搜索的时候，将使用member属性来搜索某个组的所有子组。

• 分页搜索：使用扩展API对LDAP服务器进行搜索，建议保留默认配置。

• 页面大小：LDAP分页时返回的大小，0表示无限制，建议保留默认配置。

• 大小限制：同步LDAP时的size limit选项，这里建议保留默认配置。

步骤7.在AC上配置认证策略。在[接入管理/接入认证/PORTAL认证/认证策略]界面，点击<新增>按钮新建一条Portal认证策略。

• 认证范围：按实际需求配置策略生效的IP地址范围。

• 认证方式：选择密码认证，并在认证服务器栏勾选已配置好的LDAP服务器。

其他的功能项按需配置即可，最后提交并保存配置。

步骤8.在PC的认证界面使用LDAP服务器存储的用户名密码认证，在AC上查看该用户能否成功入网。

6.2.1.2.6.Radius服务器

用户使用Radius第三方认证时，都需要在[外部认证服务器]页面先添加对应的Radius服务器，并设置相关信息。

• 服务器名称：用于设置Radius服务器名称。

• IP地址：填写Radius服务器的IP地址。

• 认证端口：设置Radius服务器的认证端口，默认是1812。

• 超时时间：设置认证请求的超时时间。

• 共享密钥：设置Radius协商密钥。

• 采用协议：设置Radius协商协议，不加密的协议PAP、质询握手身份验证协议、Microsoft CHAP、Microsoft CHAP2、EAP_MD5。

• 编码：支持选择UTF-8或GBK编码格式。

6.2.1.2.7.POP3服务器

内网用户使用POP3单点登录的认证方式时，需要在[外部认证服务器]页面先添加对应的POP3服务器，并设置相关信息。

服务器名称：填写POP3服务器名称。

POP3服务器配置：用于设置POP3服务器的IP地址、认证端口和超时时间。

6.2.1.2.8.**OA账号认证**

现在企业微信、阿里钉钉和口袋助理在企业里使用越来越普遍，使用企业微信的用户在企业微信里相当于已经有一套完整的组织结构和认证体系，希望AC可以借助企业微信实现上网的认证。AC提供和企业微信结合认证的方式来完成认证，上网的时候弹出二维码，通过手机微信进行扫码授权，实现认证。在手机端，弹出认证页面，直接拉起微信进行授权认证。

Oauth2.0认证方式的应用，AC内置OA账号认证支持企业微信、阿里钉钉和口袋助理三种认证方式。

企业微信认证

企业微信参数配置流程：

1. 登录企业微信管理后台；
2. 选择“我的企业”，获得企业ID，填入appid栏；
3. 选择“应用与小程序”；
4. 获取AgentId、secret,分别填入企业id，appsecret。

步骤1.配置开发者平台， 登录企业微信管理后台：

https://work.weixin.qq.com/wework_admin/loginpage_wx?redirect_uri=https://work.weixin.qq.com/wework_admin/frame#profile

步骤2.选择“我的企业”，获取企业ID，填入AC设备认证服务器的AppID栏。

步骤3.选择“应用与小程序”，自建中点击“创建应用”，应用名称填“我要上网”。

步骤4.点击进入“我要上网”。

步骤5.获取AgentId、secret分别填入AC设备认证服务器的企业id栏和Appsecret栏。

步骤6.点击进入“网页授权及JS-SDK”，填入“oauthservice.net”。

步骤7.启用“企业微信授权登录”，填入授权回调域名“oauthservice.net”。

步骤8.启用“工作台应用主页”，填入：

https://open.weixin.qq.com/connect/oauth2/authorize?appid=ww9c6d66e15efc420c&redirect_uri=http%3A%2F%2Foauthservice.net%2Fac_Portal%2Foauth_callback.html&response_type=code&scope=snsapi_base&state=qywechat-#wechat_redirect；其中AppID替换为步骤1获取的AppID。

步骤9.勾选“在微工作台中始终进入主页”。

步骤10.企业微信配置参数获取完成，在[接入管理/接入认证/认证服务器]，点击<新增>[OA账号认证/企业微信]，勾选启用，填写名称、描述。

步骤11.对接参数设置根据前面步骤获取填入。

步骤12.在[接入管理/接入认证/PORTAL认证/认证策略]，点击<新增认证策略>，填写认证范围，引用配置好的企业微信服务器，点击<提交>，完成配置。

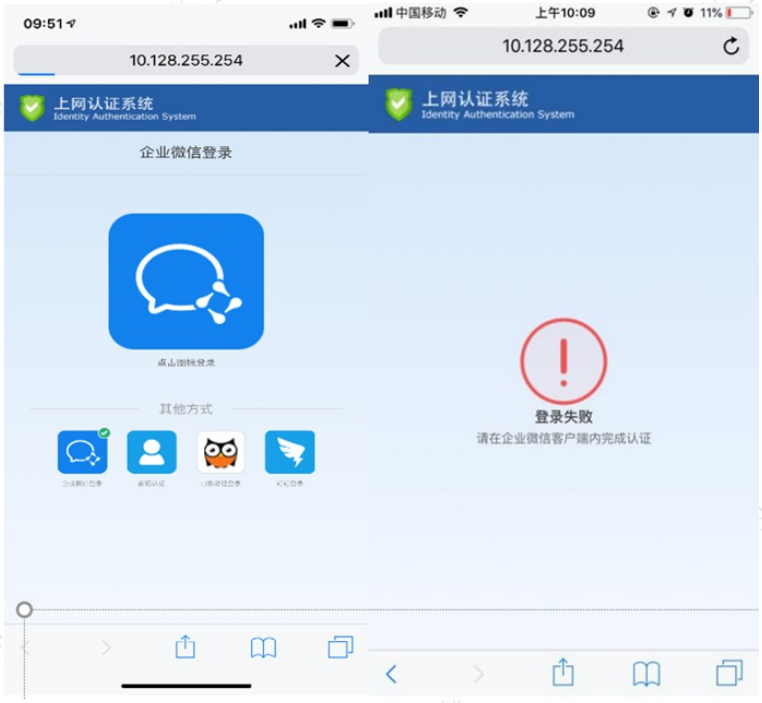
步骤13.效果呈现：PC端效果，点击认证方式图标。

步骤14.手机端跳转到二维码扫描页面，使用手机企业微信扫描二维码（手机不必要接入网络）。

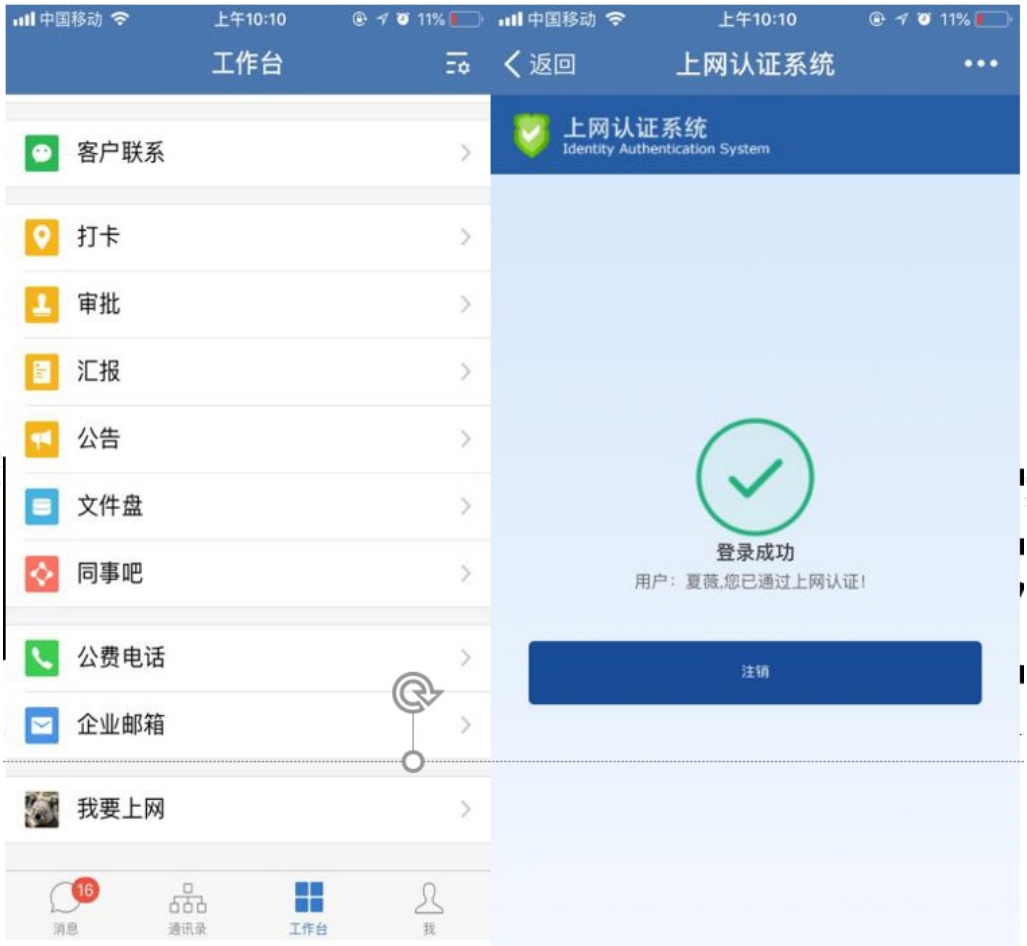
步骤15.手机企业微信扫码认证后，跳转到访问前页面。

步骤16.在[全网监控/入网用户管理]可查看通过认证用户列表。

移动端效果：手机接入wifi后，用浏览器打开一个页面，重定向到认证页面，点击企业微信认证，跳转到登录失败页面，并提醒在企业微信客户端内完成认证。



手动进入企业微信App，点击下方导航栏的“工作台”，拉倒最下面，看到“我要上网”点击，完成认证。完成后，可以上网。



阿里钉钉认证

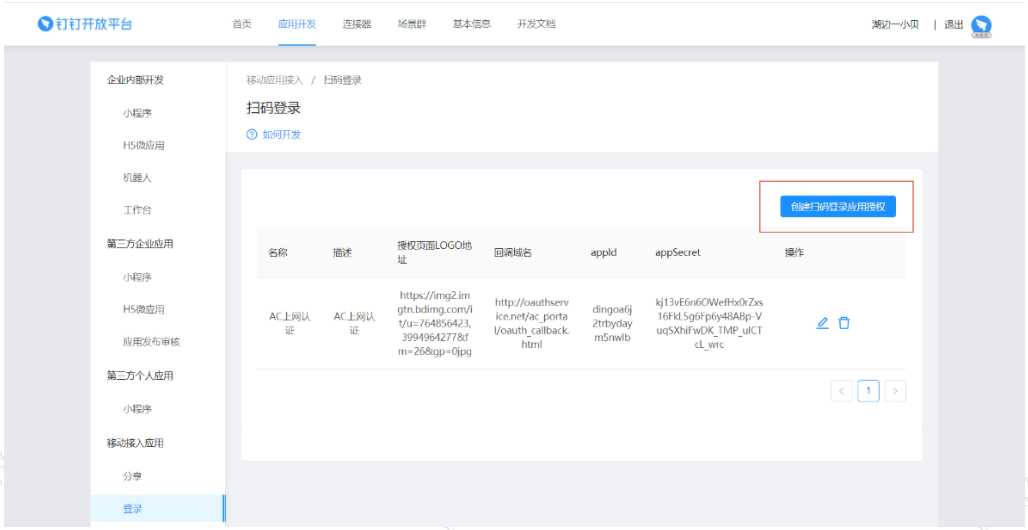
钉钉认证配置流程：

1. 阿里钉钉认证开发平者平台配置；
2. AC认证配置；
3. 效果演示。

配置步骤

步骤1.登录首页获取企业ID信息。

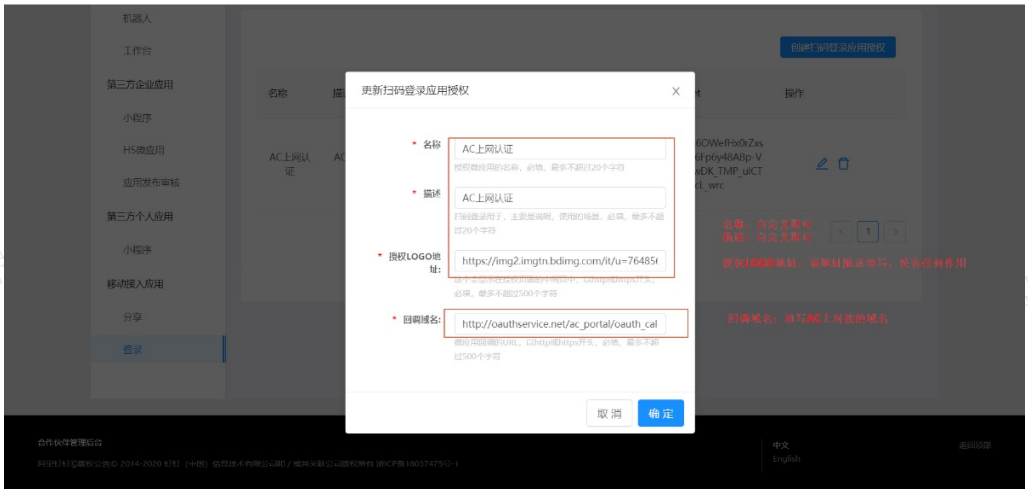
步骤2.在“应用开发”标签下进入“移动应用接入”，点击“登录”；创建扫码登录认证授权。



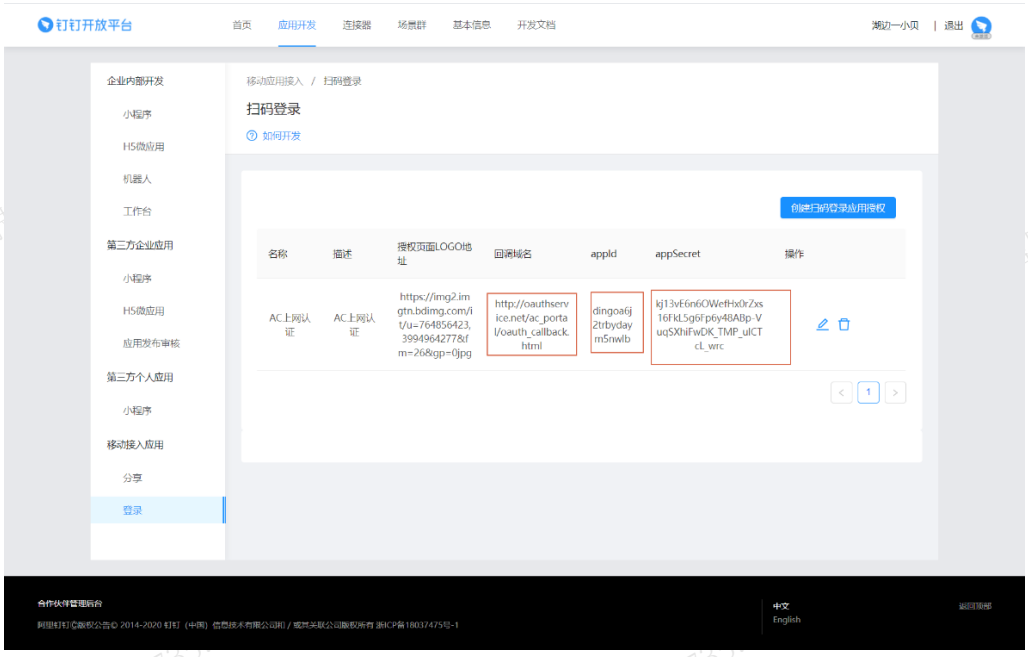
步骤3.**名称**：自定义，例如AC上网认证；**描述**：自定义，例如AC上网认证。

授权LOGO地址：无特殊作用，可以任意填写，https://img.com

回调域名：AC设备的钉钉认证回调地址， http://oauthservice.net/ac_Portal/oauth_callback.html



步骤4.创建成功。



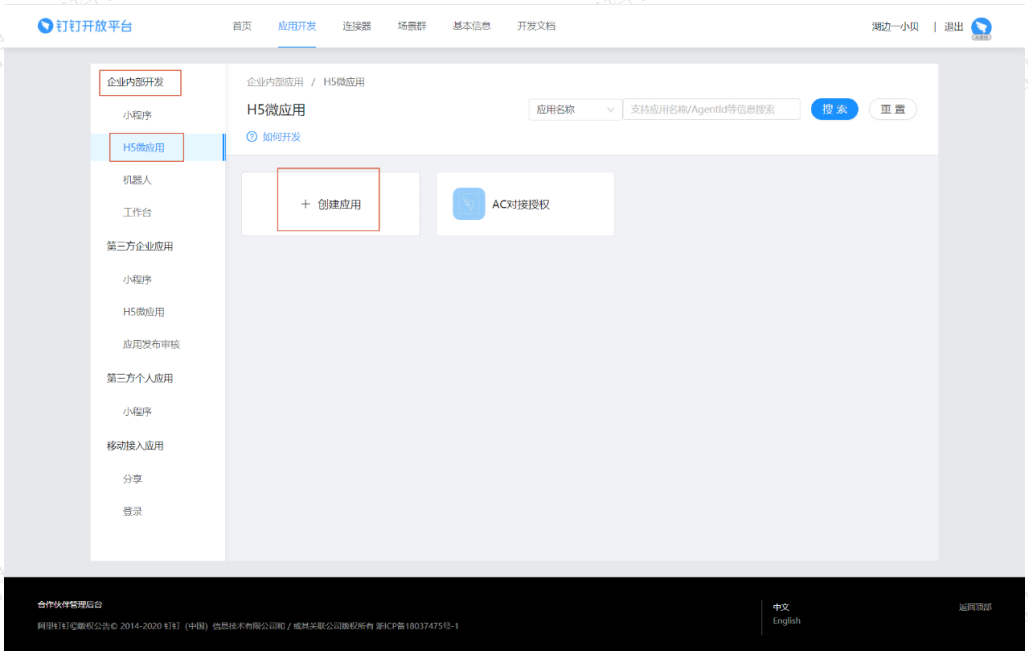
收集钉钉上的appID和appSecret，该信息主要用于AC认证的回调。本例中：

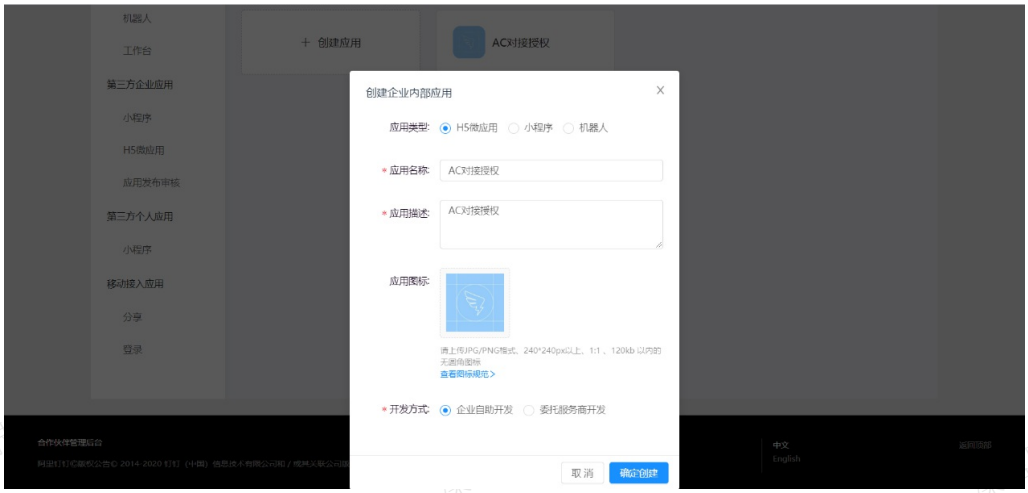
appid：dingoa6j2trbydaym5nwlb

appSecret：kj13vE6n6OWefHx0rZxs16FkL5g6Fp6y48ABp-VuqSXhiFwDK_TMP_ulCTcL_wrc

步骤5.在“应用开发”标签下进入“企业内部开发”，点击“H5微应用”；创建AC对接授权

- 应用名称：**自定义，例如AC对接授权**
- 应用描述：**自定义，例如AC对接授权**
- 开发方式：**企业自助开发**

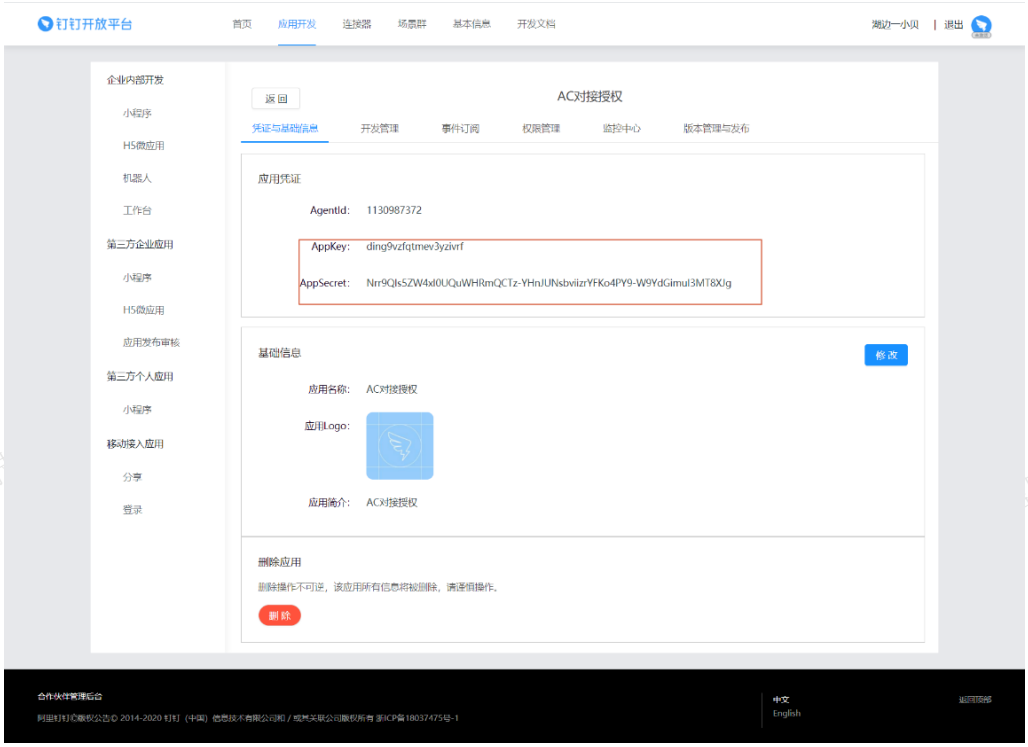




步骤6.创建H5微应用成功后，点击应用，在应用的“凭证与基本信息”->“应用凭证”中收集应用的appkey、appsecret，本例中：

AppKey：ding9vzfqtmev3yzivrf

AppSecret：Nrr9QIs5ZW4xI0UQuWHRmQCTz-YHnJUNsbviizrYFKo4PY9-W9YdGimuI3MT8XJg



步骤7.在H5微应用中，“开发管理”设置上网行为管理的互联网出口地址。

- 开发模式：**开发应用**
- 服务器出口IP：**该地址为AC设备自身出去上网的互联网IP地址**
- 应用首页地址：**自定义，例如https://www.dingtalk.com**

步骤8.在H5微应用配置AC用户认证的范围和用户认证所需的权限，在“权限管理”模块，添加接口权限，需要新增：通讯录只读和通信录编辑权限，邮箱等信息可选。

如上步骤整理完成之后收集信息如下，配置到AC设备钉钉对接认证模块即可：

CorpId:dingf8e689809c2fc7a44ac5d6980864d335

appid:dingoa6j2trbydaym5nwlb

appSecret:kj13vE6n6OWefHx0rZxs16FkL5g6Fp6y48ABp-VuqSXhiFwDK_TMP_ulCTcL_wrc

AppKey：ding9vzfqtmev3yzivrf

AppSecret：Nrr9QIs5ZW4xI0UQuWHRmQCTz-YHnJUNsbviizrYFKo4PY9-W9YdGimuI3MT8XJg

步骤9.认证服务器配置：只需要填写appid、appsecret参数和企业ID；如果有获取组织结构需求，勾选“自动获取用户所属组”配置起始路径、appkey和appsecret。

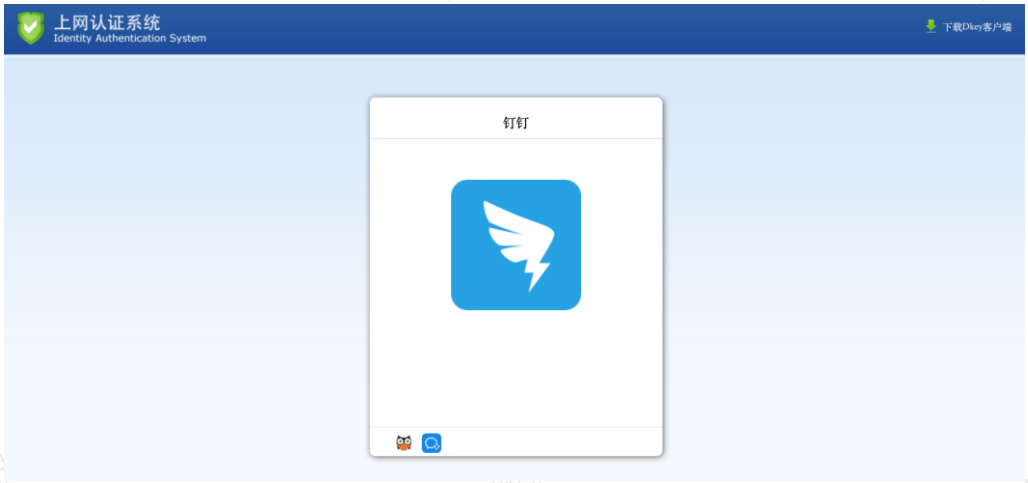
步骤10.在[用户认证与管理/用户认证/认证策略]，新增认证策略，填写认证范围，引用配置好的阿里钉钉认证服务器。

注意事项：

钉钉认证属于第三方认证，用户以oauth认证方式上线，默认以钉钉的用户名为登录名，钉钉的用户名和本地用户的登录名不能发生冲突。

步骤11.[接入管理/接入认证/PORTAL认证/认证策略],点击<新增认证策略>，填写认证范围，引用配置好的阿里钉钉认证服务器，点击<提交>，完成配置。

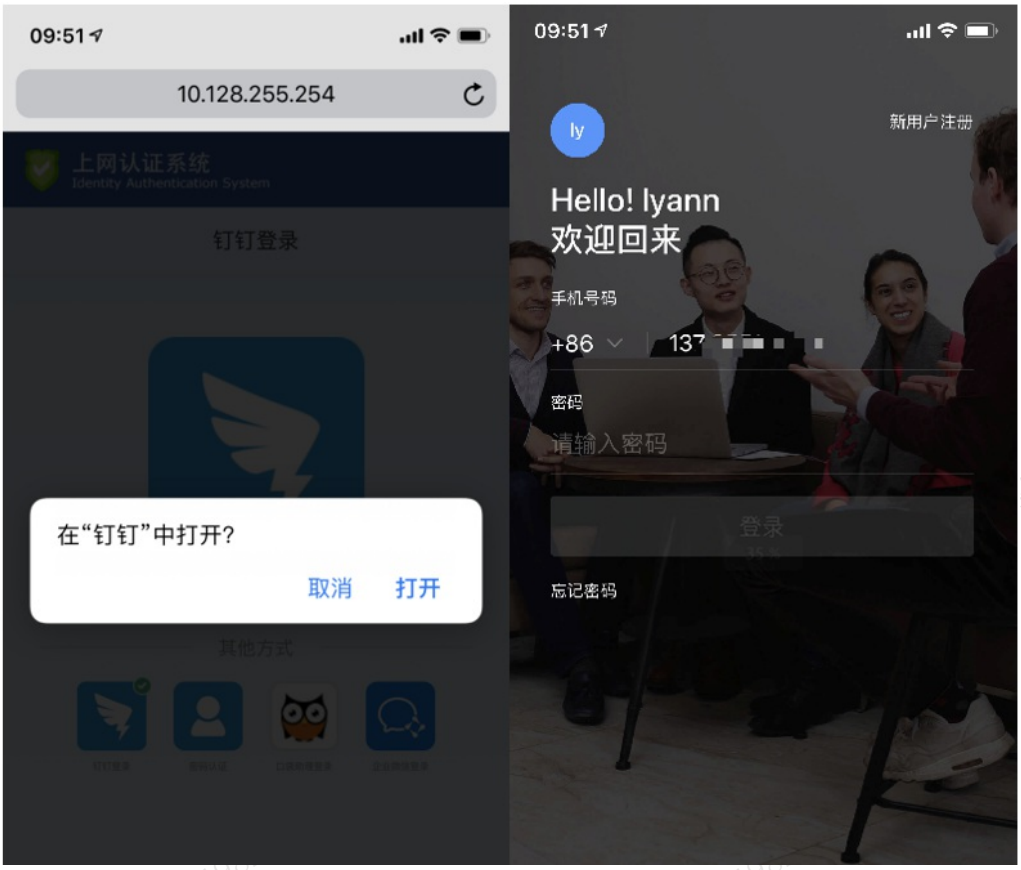
步骤12.效果呈现：PC端效果：点击认证方式图标。



步骤13.使用手机阿里钉钉扫描二维码登录（手机不必须要接入网络）。

步骤14.手机钉钉扫二维码完成认证,跳转到访问前页面。

步骤15.移动端效果：手机接入WIFI后，用浏览器打开一个页面，重定向到认证页面，点击钉钉认证，唤起阿里钉钉app，在app完成登录后，完成认证。



步骤16. 完成认证后，在线用户列表看到上线情况。

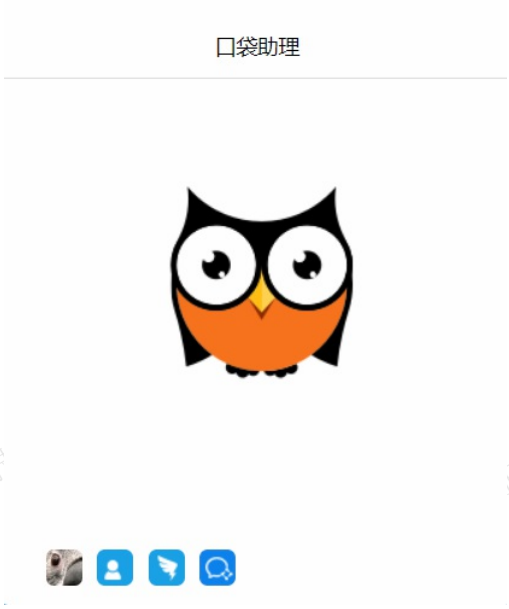
口袋助理认证

口袋助理未提供对外的开发者平台，有认证需求联系深信服售后400或区域获取参数；

步骤1.在AC上配置OA账号认证服务器，服务器参数需在第三方平台注册授权应用获取，禁用自动获取用户所属组；

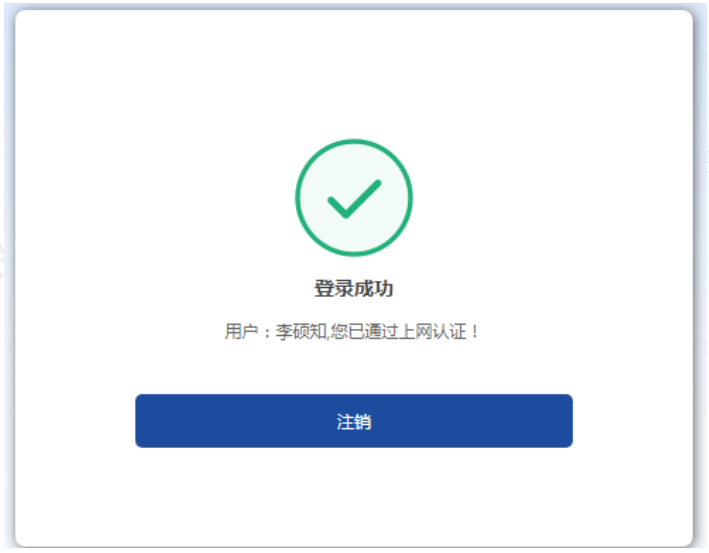
步骤2.对口袋助理的登录域名加入全局排除地址（认证前流量未放通）

步骤3.认证过程：根据认证策略配置，认证页面提供OA账号认证方式供用户选择。



步骤4.用户选择认证方式后，跳转到OA账号认证页面完成认证。

步骤5.认证完成后认证平台会通过在平台填写的URL参数回调给AC，AC可获取用户在第三方平台的认证信息，在AC上登录上线。



步骤6.认证后效果：在线用户所属组即[认证策略/认证后处理/非本地/域用户使用该组上线]配置的组。

步骤7.移动端效果：口袋助理与另外两个不同的是不需要拉起app，浏览器访问网页点口袋助理认证图标跳转到口袋助理登录页面，输入手机号和密码即可完成认证。

6.2.1.2.9.社交账号认证

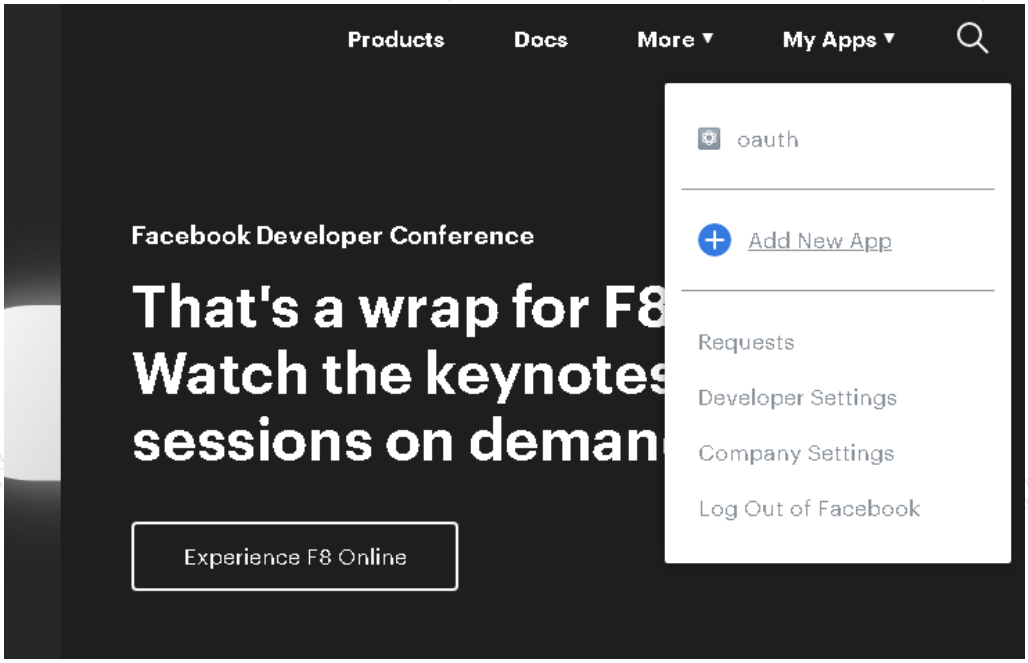
国外很多网站使用Facebook账号、Twitter账号、Google账号登录。这种社交账号对用户来说非常方便，不需要注册账号即可登录。AC在公共上网场景里也面临类似需求，用户希望能用社交类账号进行认证，特别是在海外，Facebook账号、Twitter账号、Google账号登录非常方便，满足公共上网场景里使用社交账号的需求。设备支持结合Facebook、Gmail、Line、Twitter这四种社交账号实现认证。

[接入管理/接入认证/PORTAL认证/认证服务器]，点击新增<社交账号认证服务器>。

Facebook账号认证

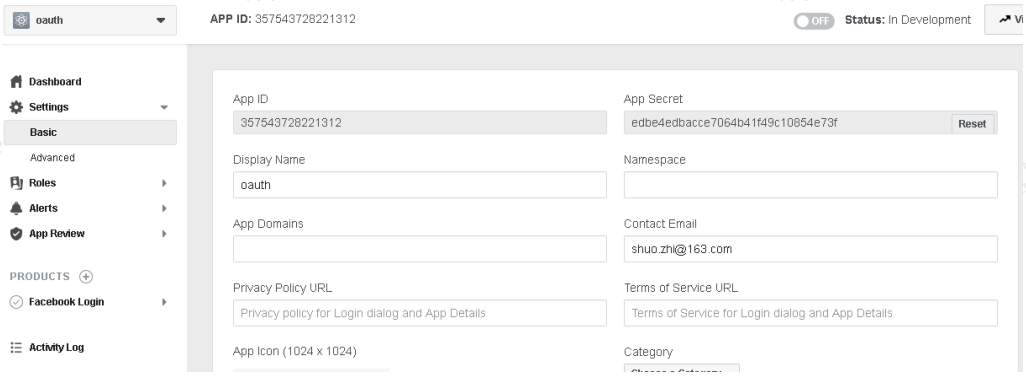
步骤1.配置开发者平台，Facebook开发者应用注册网址：https://developers.facebook.com

步骤2.Add New App，填入名称和邮箱。

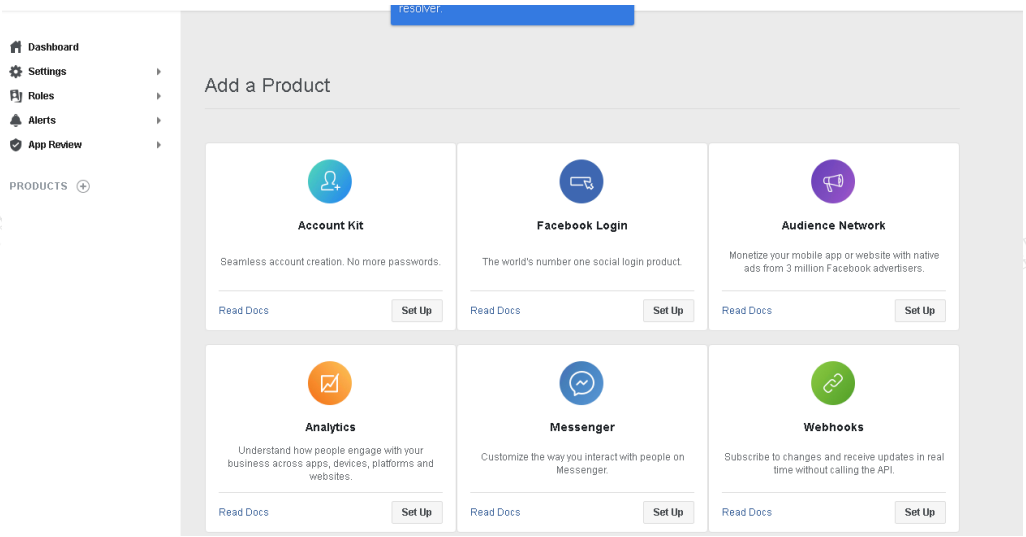


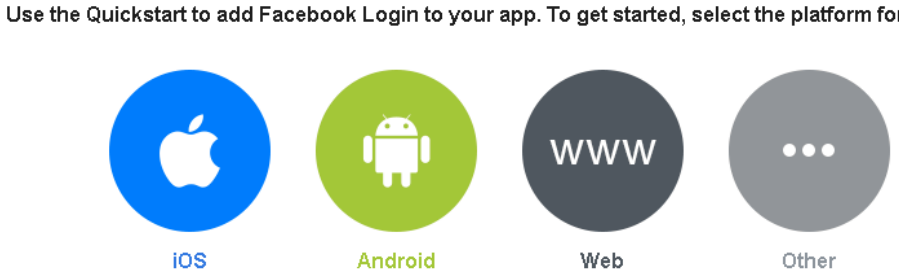
步骤3.进入Setting选择Basic，获取AppID 和AppSecret填入appid、appsecret中。

步骤4.填入Privacy Policy URL：Privacy URL意思是填自己公司的主页之类的，实际上这个参数在Oauth认证里面用不到，随便写一个URL也可以。

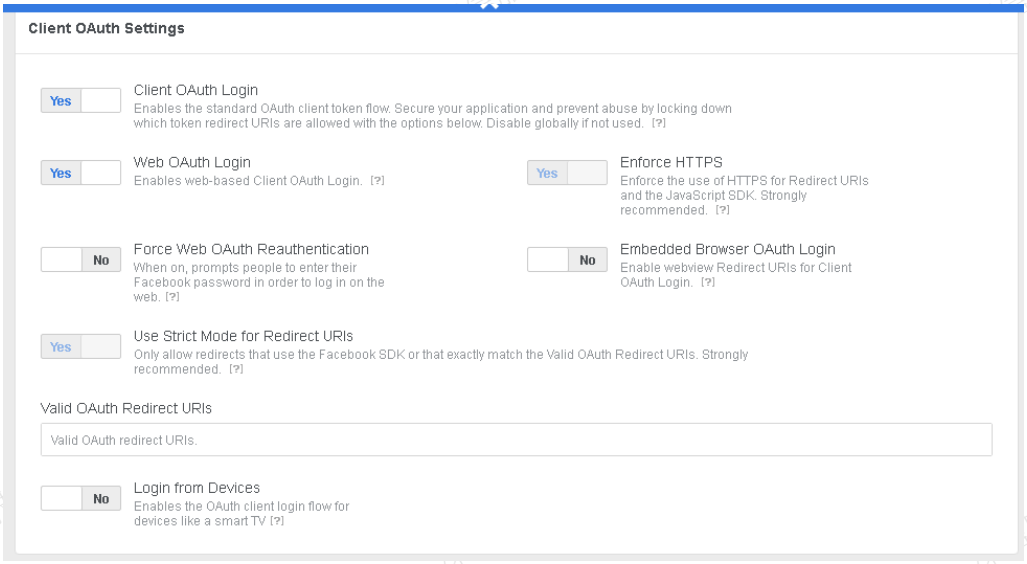


步骤5.添加“Facebook Login”产品，选择“Web”。





步骤6.进入设定，填入Valid OAuth Redirect URIs：https://oauthservice.net:444/ac_Portal/oauth_callback.html（在AC控制台复制）。



最后，填上隐私策略网址，然后点击对外开放。

步骤7.社交账号认证（FaceBook）服务器配置，策略名称和Appid和AppSecret参数。

步骤8.[接入管理/接入认证/PORTAL认证/认证策略],点击<新增认证策略>，填写认证范围，引用配置好的facebook认证服务器，点击<提交>，完成配置。

步骤9.效果呈现，点击认证方式图标。

步骤10.输入facebook的用户名密码。

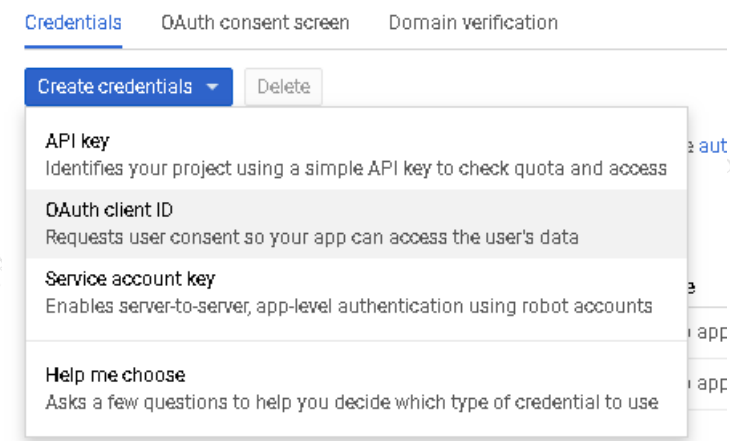
步骤11.完成认证效果。

步骤12.在线用户显示上线情况。

Gmail账号认证

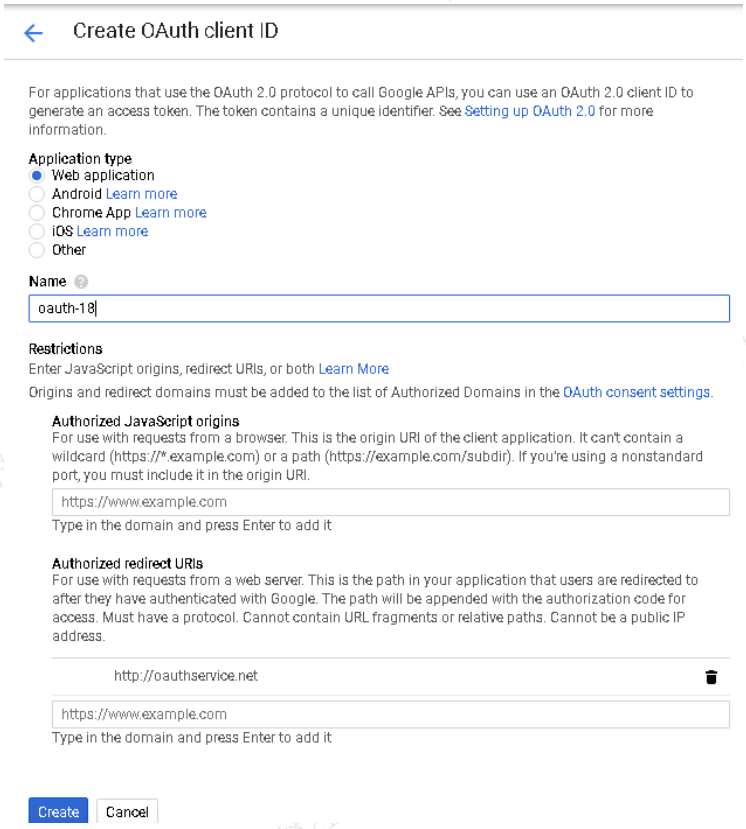
步骤1.配置开发者平台：登录google开发者平台：https://console.developers.google.com

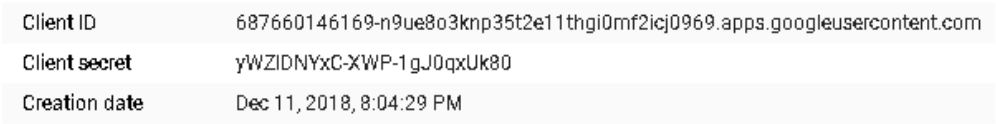
步骤2.进入凭据，创建凭据，选择“Oauth客户端ID”。



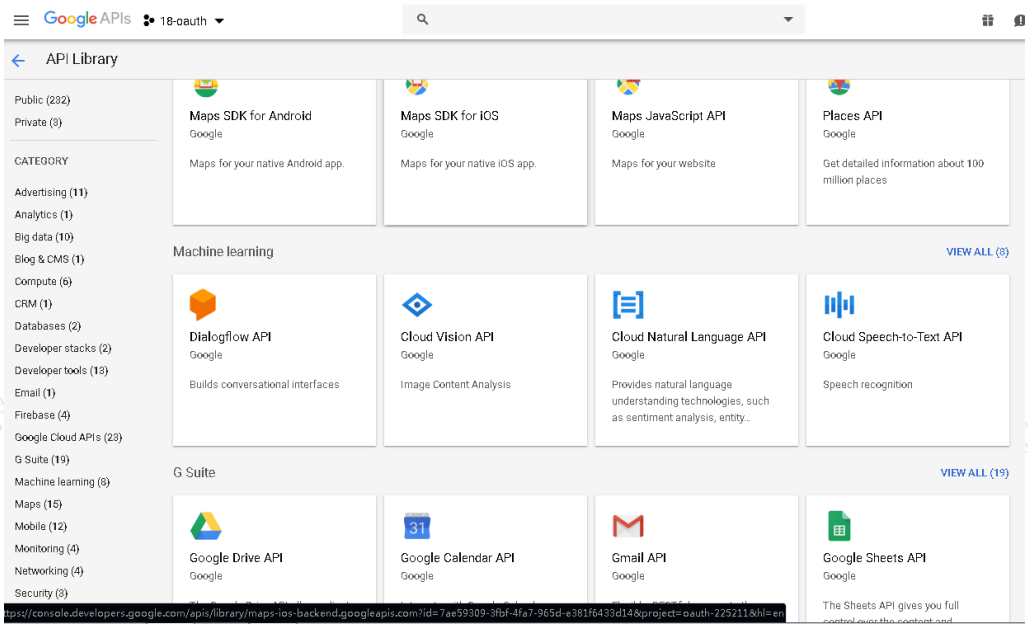
步骤3.选择“网页应用”，填入已获授权的重定向URI：

http://oauthservice.net/ac_Portal/oauth_callback.html（建议在AC后台直接复制重定向url）。





步骤4.点击库， 在API库中选择“Gmail API”，点击<启用>。



步骤5.认证服务器配置，需要填写名称和描述appid和appsecret参数将创建后的用户端ID，用户端密钥填入appid，appsecret。

步骤6.[接入管理/接入认证/PORTAL认证/认证策略],点击<新增认证策略>，填写认证范围，引用配置好的Gmail认证服务器，点击<提交>，完成配置。

步骤7.效果呈现,点击认证方式图标。

步骤8.输入账号密码，点击<提交>。

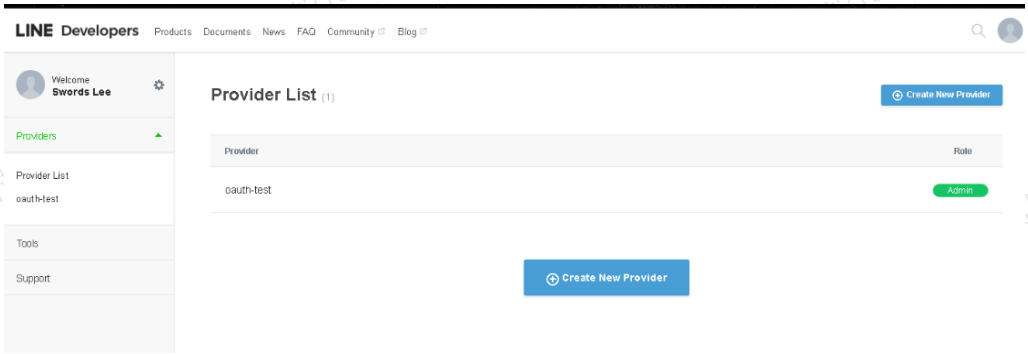
步骤9.完成认证，跳转到访问前页面。

步骤10.在线用户上线情况。

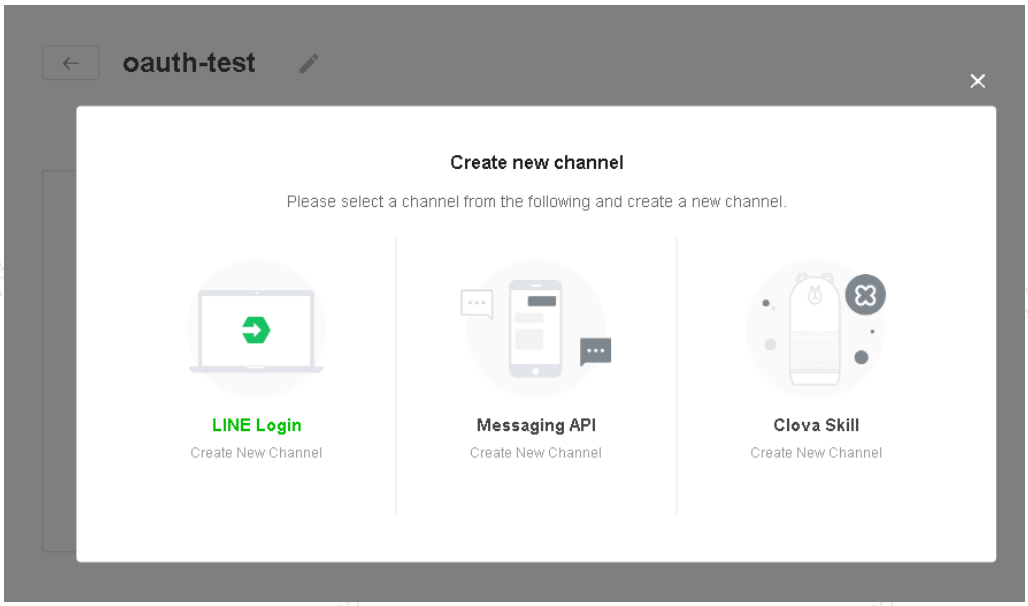
Line账号认证

步骤1.登录Line开发者平台：https://developers.line.biz/console/。

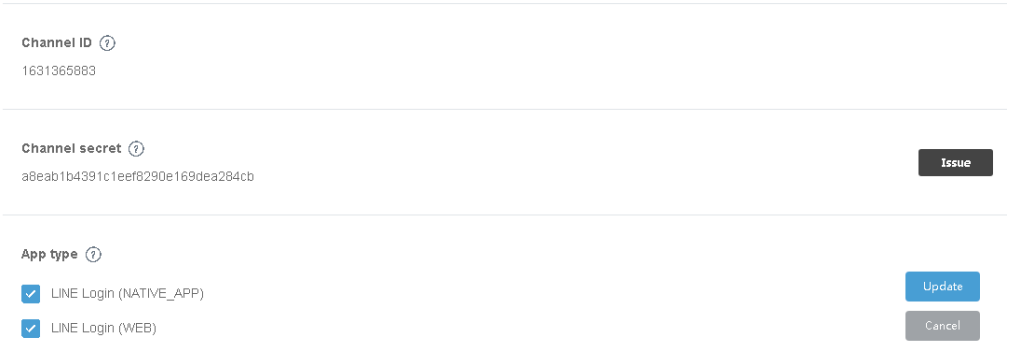
步骤2.进入providers点击，Create New Provider，按照指引完成provider创建。



步骤3.进入创建的provider，点击create channel，选择LINE Login，按照指引完成channel创建。

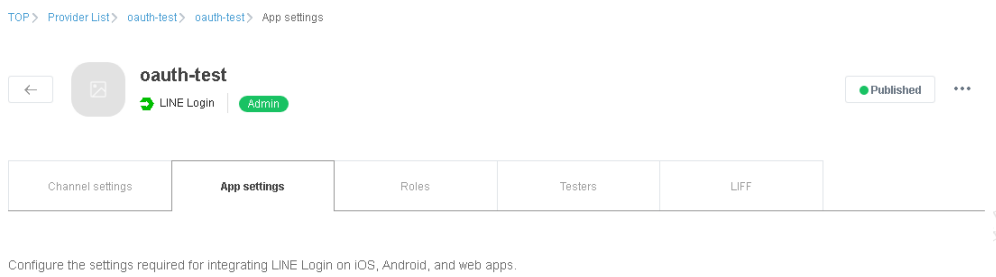


步骤4.点击进入新建的channel，在channel setting下获取Channel ID、Channel secret 填入appid、appsecret中，并勾选App type下LINE Login(NATIVE_APP)， LINE Login(WEB)。



步骤5.在App Setting下设置填入Callback URL，可在AC控制台复制。

步骤6.将channel 状态改为published。



步骤7.AC认证配置：认证服务器配置：只需要填写AppID和AppSecret参数。

步骤8.[接入管理/接入认证/PORTAL认证/认证策略]，点击<新增认证策略>，填写认证范围，引用配置好的Line认证服务器，点击<提交>，完成配置。

步骤9.效果呈现，点击认证方式图标。

步骤10.点击line图标跳转到登录line页面，输入账号密码。

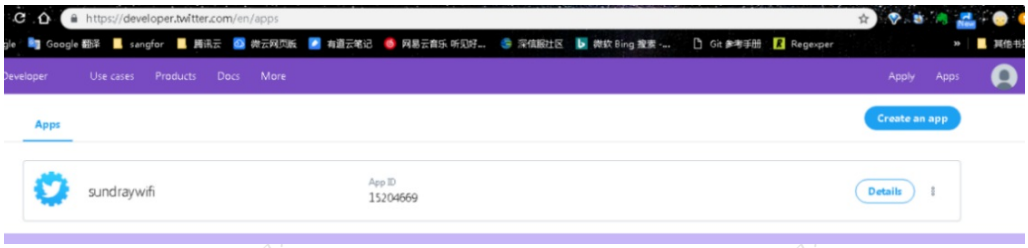
步骤11.认证成功后，跳转到认证前访问页面。

步骤12.设备在线用户上线。

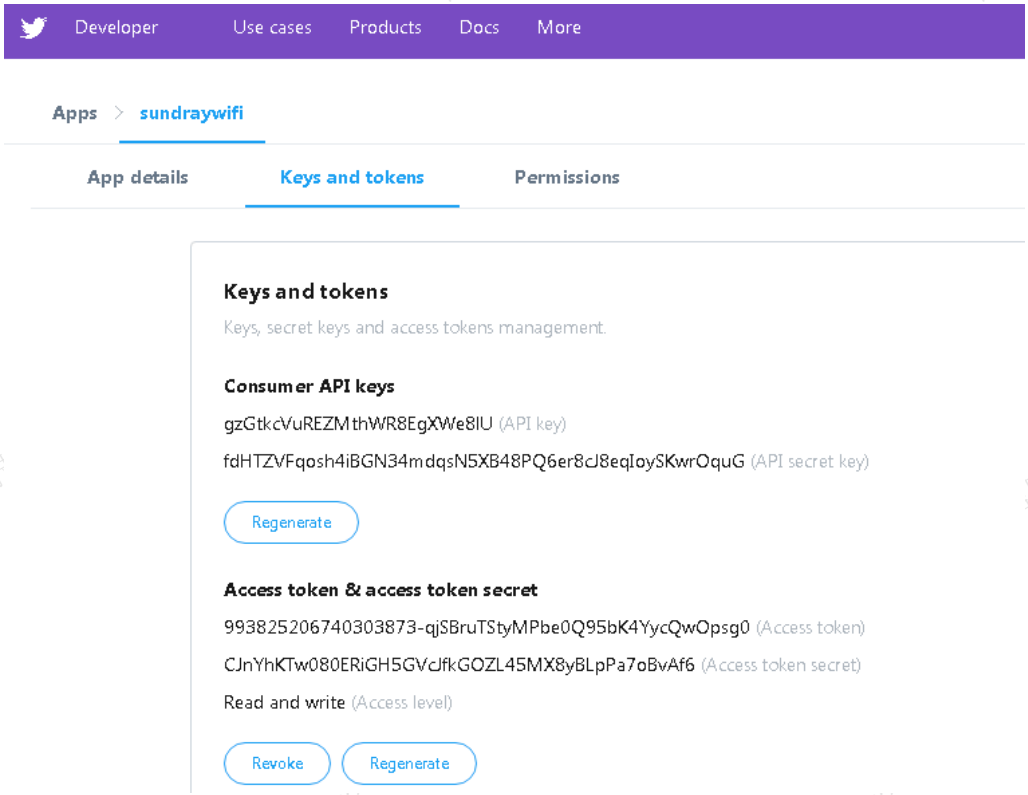
Twitter账号认证

步骤1.登录twitter开发者平台:https://developer.twitter.com/en/apps

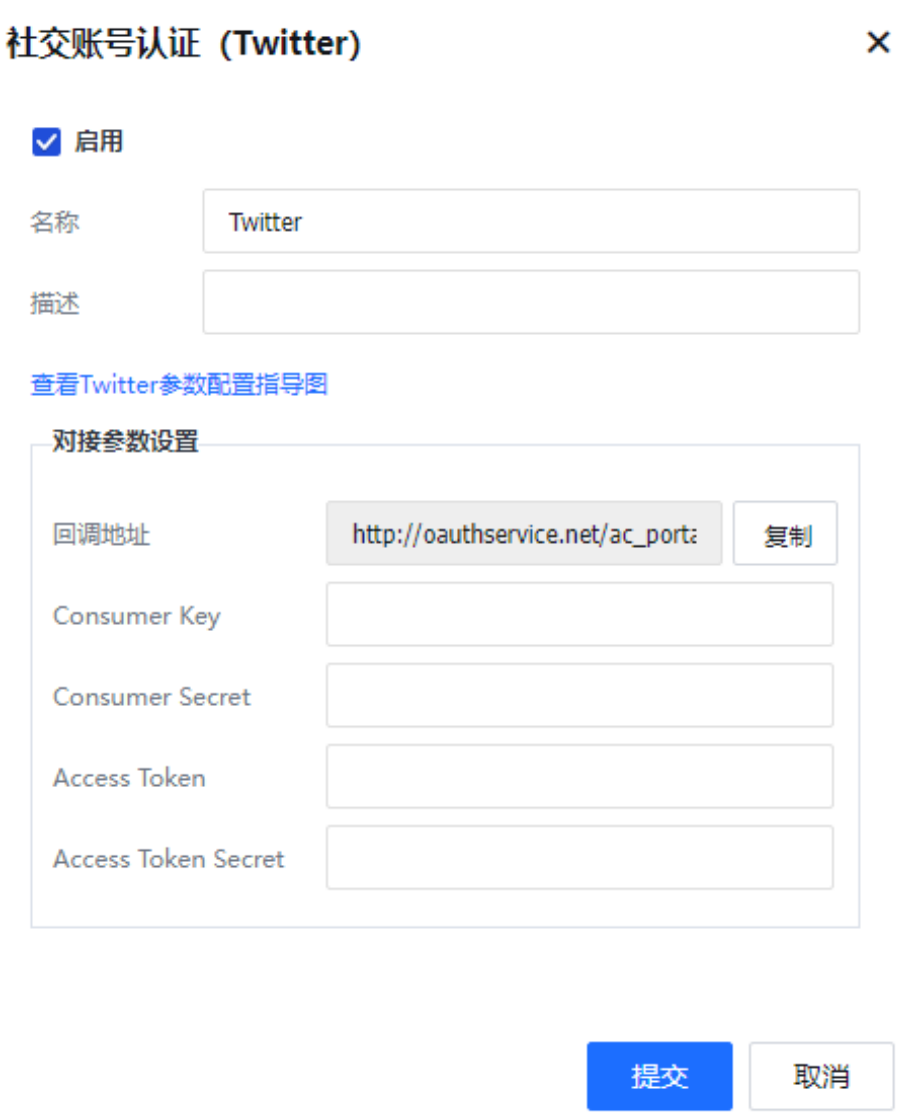
步骤2.进入点击detail进入app。



步骤3.点击“Keys and tokens”获取应用参数。

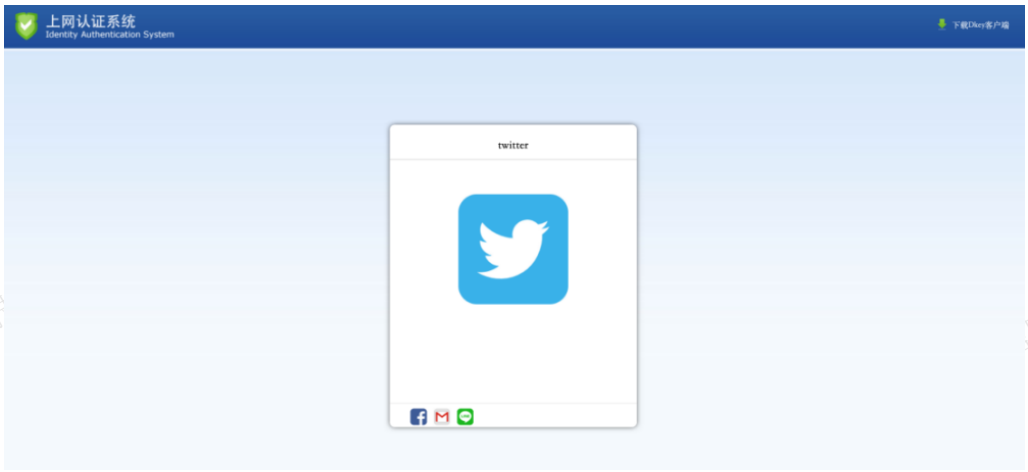


步骤4.AC认证配置：认证服务器配置：填写参数。

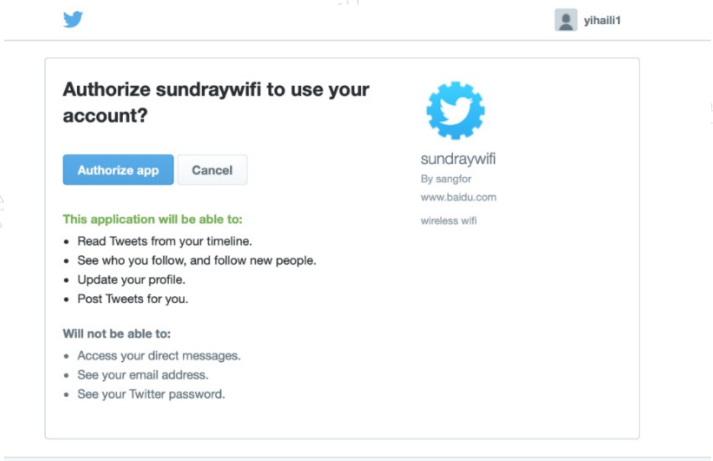


步骤5.[接入管理/接入认证/PORTAL认证/认证策略]，点击<新增认证策略>，填写认证范围，引用配置好的Twitter认证服务器，点击<提交>，完成配置。

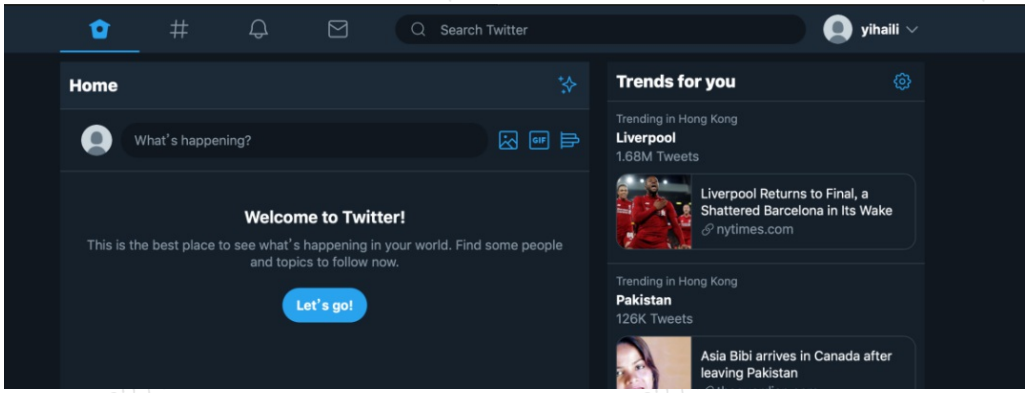
步骤6.效果呈现：点击认证方式图标。



步骤7.输入Twitter账号完成认证。



步骤8.认证后，正常使用Twitter。



步骤9.在线用户上线。

6.2.1.2.10.数据库服务器

内网用户使用数据库单点登录的认证方式时，需要在外部认证服务器页面先添加对应的数据库服务器，并设置相关信息。

勾选启用该外部认证服务器，该功能才会生效。

- 服务器名称：定义方便区分的服务器名称。

• 数据库类型：择数据库的类型，支持DB2，ORACLE，MS SQL和MYSQL。

• 服务器地址和端口：写数据库服务器的地址和数据库监听端口。

• 数据库编码：选择数据库的编码类型，提供UTF-8、GBK、BIG5三种选择。

• 用户名：填写数据库的用户名。

• 密码：填写数据库的密码。

• 数据库名：写数据库名称。

• 超时：设备连接数据库服务器取数据时，多久没有返回数据则视为超时，默认值60s，可根据服务器的负载和用户数酌情调整。

• 测试有效性：测试设备跟服务器的连通性及上述配置的有效性。

6.2.1.2.11.**H3C CAMS服务器**

内网用户使用H3C CAMS单点登录的认证方式时，需要在外部认证服务器页面先添加对应的服务器，并设置相关信息。

勾选启用该认证服务器。

• 服务器名称：自定义一个便于区分的服务器名称。

• 服务器地址：写服务器的地址及其端口号，格式为IP:端口或服务器URL地址。

• 数据库编码：择数据库的编码类型：UTF-8、GBK、BIG5，数据库编码决定以什么编码显示用户名等字符，若编码选择不正确，则可能出现用户名乱码。

• 用户名和密码：填写H3C CAMS系统管理员用户的名称和密码。

• 超时：设备连接H3C CAMS系统所消耗的时间，可根据服务器的负载调整，建议使用默认值60s。

• 测试有效性：测试设备跟服务器的连通性及上述配置的有效性。

6.2.1.2.12.第三方认证系统

CAS认证

勾选启用该认证服务器。

• 服务器名称：**自定义一个便于区分的服务器名称。**

• URL：**填写服务器的URL，请参考“https://IP:8443/cas/login”。**

• 关键字：**用来识别回包关键字，提取用户名。默认格式：**

cas:serviceResponse>cas:authenticationSuccess>cas:user

• 校验版本：**可以选择cas2.0或cas3.0。**

Oauth认证

设备内置了7个Oauth的认证方式，如果需要实现除这7种以外的Oauth认证，可以在[认证服务器/第三方认证系统/Oauth]认证服务器进行配置。

在[接入管理/接入认证/PORTAL认证/认证策略]，点击<新增认证策略>，填写认证范围，引用配置好的Oauth认证服务器。

SAML2.0认证

设备支持通过SAML2.0协议与企业内部的身份认证系统集成，实现单点登录。入网用户在内部的身份认证系统完成认证后即可单点登录AC，在AC上完成用户上线。

勾选启用该认证服务器。

LdP Login Url：IDP认证页面Url,用于跳转至IDP的认证页面。

LdP Entity ID：IDP标识符，用于AC校验IDP身份的合法性。

SP Entity ID：SP标识符，用于IDP校验AC身份的合法性。

认证后跳转地址：AC接收认证响应报文接口，由AC提供至IDP。

指定签名位置：用于指定签名计算方式，此设置AC和IDP两端需要保持一致。

说明：

1. 目前只支持对接微软SAML2.0协议。

2. AC指定签名只支持assertion或response，不支持assertion和response。

3.只支持pem,der,cer，crt后缀证书。

4.支持SHA-1签名算法和SHA-256签名算法

单点登录

6.2.1.3.1.**微软AD域**

如果用户的网络中已有一台微软AD域服务器做用户管理，内网用户登录电脑系统都是使用域账号登录，可

以采用域单点登录的方式，在内网用户登录到域之后就通过设备的认证，即终端用户登录域即可上网，无需通过设备再次认证。域单点登录有四种办法可以实现：

• 通过域自动下发脚本登录：**通过在域服务器上配置登录（logon.exe）和注销（logoff.exe）脚本，在用户登录域或注销域时通过下发的域策略执行登录或注销脚本，执行脚本的同时完成用户在设备上的登录和注销**。

• 通过AC本身程序自动登录（ADSSO登录）：**AC设备内置一个单点登录客户端程序ADSSO。启用这种方式时，主动检测AD域上终端用户登录域的事件日志（事件ID为672，540，4624），检测到有用户登录的日志后即自动通过AC认证。**

• 集成windows身份登录（IWA登录）：**在windows域环境下普遍支持的一种认证方式。通过这种方式实现的单点登录，需要先将AC设备和内网电脑都加入到域，当内网电脑打开网页时会自动访问AC并提交身份凭证，从而实现单点登录。**

• 监听口监听登录信息登录：**通过监听PC登录域服务器的数据，从监听到的数据中获取用户登录的信息，从而实现的单点登录。监听模式的单点登录无需在域服务器上安装任何组件，但要求内网电脑登录域的数据经过设备或者是通过监听口镜像到设备。且只能监听登录信息，不能监听注销信息。**

以上几种方式可以单独使用，也可以同时使用，它们之间不冲突，同时使用也可以增加单点登录的成功率。具体配置参考接入认证AD域典型案例章节。

6.2.1.3.2.**Radius**

当用户环境中存在Radius服务器，并且Radius认证和计费的数据包经过AC设备时，可以启用Radius单点登录认证方式，认证成功以Radius的用户名上线。

当第三方Radius服务器认证和计费的数据包不经过AC，则需要通过交换机做镜像流量的方式将Radius计费报文镜像到AC的镜像口。当AC通过镜像流量抓取到Radius计费报文的目的IP后，PC通过Radius认证则成功通过AC认证，AC在线用户列表里可以看到认证的账号以及IP。

⚠ 注意 ：

1．必须将Radius的计费报文镜像给AC。如果镜像的是Radius认证报文则需要考虑用户的使用场景，只有Portal认证时Radius认证报文里才会携带IP地址，802.1x认证的Radius认证报文是不携带IP地址的。而Radius计费报文不管是Portal认证还是802.1x认证均会携带用户名和IP地址。

2．如果AAA认证场景下未使用计费功能，可以开启计费功能把Radius计费报文发送给AC，即把AC当作Radius的计费服务器实现Radius单点登录。

操作步骤

步骤1.在[接入管理/接入认证/PORTAL认证/认证策略]，点击<新增>认证策略，勾选启用，填写名称、描述和认证范围。

步骤2.认证方式选择单点登录，已开启单点登录方式：显示当前已开启的方式，可点击<配置单点登录>跳转到单点登录页面。单点登录失败的用户还能选择：不需要认证，自动上线、密码认证、跳转到提示页面、跳转到CAS服务器。推荐选择密码认证方式，也可根据实际需求选择。

步骤3.点击<配置单点登录>跳转到单点登录页面，勾选[启用Radius单点登录]。如果Radius认证和计费的数据包不经过AC，则需要在AC上设置镜像口，并把这部分数据通过镜像口镜像到AC上。

步骤4.在Radius服务器地址列表中填写Radius服务器的地址，如果AC作为Radius服务器，则服务器为AC的地址。

• 读取Radius属性，并自动赋值给用户的自定义属性：**Radius用户存在一些属性值，AC上也可以设置用户的属性值，如果Radius用户认证的同时也需要把属性带到AC上，则需要勾选此项。**

• Radius属性：**设置需要读取的Radius属性。**

• 赋值给用户的自定义属性：**设置需要把上面的Radius属性赋值到AC的哪个自定义属性上。**

步骤5.认证后处理，默认设置即可，点击<提交>配置完成。

步骤6.Radius计费包抓取成功，传递用户名至AC，AC在线用户列表显示用户名，认证方式单点登录。

6.2.1.3.3.**Proxy**

如果用户网络环境中已经部署代理服务器，并且内网用户使用代理服务器上网都有账号和密码，那么可以采用Proxy单点登录的方式，在内网用户通过代理服务器的验证之后就通过设备的认证，即终端用户连接到代理服务器即可上网，无需通过设备再次认证。Proxy单点登录分监听方式和执行指定登录控件两种。

启用Proxy单点登录：开启和关闭Proxy单点登录功能。

• 监听计算机登录Proxy的数据，获取登录信息：**通过监听的方式获取用户登录proxy服务器的信息，如果用户登录代理服务器的数据不通过AC设备，需要设置监听镜像口。监听方式的Proxy单点登录配置请参见PROXY单点登录配置章节。**

• 兼容Kerberos认证方式：**若Proxy服务器为ISA服务器，并且ISA服务器采用“windows集成身份认证”方式，则需要勾选“兼容kerberos认证”方式以完成单点登录，并且该方式仅适用于登录数据包穿过AC设备的情况，不适用于镜像方式。**

• Proxy代理服务器地址列表：**填写代理服务器的IP地址。**

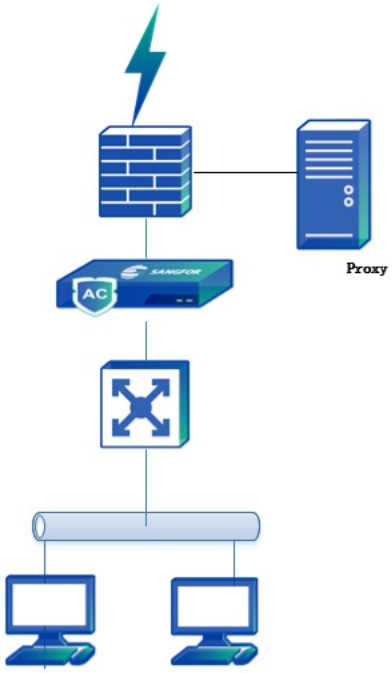
通过Proxy执行指定的登录控件，获取登录信息：需要在代理服务器上配置一个登录脚本，用户登录Proxy服务器时会自动执行该脚本，发送登录数据包到AC设备，完成登录过程。

一般适用于用户使用Proxy代理上网的环境，并且每个用户均分配了代理服务器的账号。使用Proxy单点登录的认证方式时，当用户通过Proxy服务器的验证时，同时通过设备的认证。

使用监听模式

Proxy单点登录的监听模式，也是通过监听登录数据完成单点登录的。分为两种情况：

第一种情况：Proxy服务器在外网方向，如图所示。



数据流过程如下：

1. 用户通过Proxy服务器代理上网，设备监听PC和Proxy服务器的交互。

2. PC成功经过Proxy服务器认证的同时也经过设备的认证。

操作步骤

步骤1.设置认证策略，根据需要使用单点登录的用户的IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略]新增认证策略。

步骤2.因为Proxy服务器在设备的外网方向，用户认证前需要放通访问Proxy服务器的权限，在[认证策略/认证后处理/高级选项/认证前使用此组权限]中设置一个认证前使用的组，并在权限策略中放通这个组访问Proxy服务器的权限。

步骤3.点击进入[PORTAL认证/单点登录/Proxy]页面进行配置。

步骤4.勾选[启用Proxy单点登录]，勾选[监听计算机登录Proxy的数据，获取登录信息]。

步骤5.在[Proxy代理服务器地址列表]中输入Proxy服务器的IP和监听端口，如果有多个Proxy服务器，则一行一个IP和端口，此处的端口设置Proxy认证的端口即可，如下图所示。

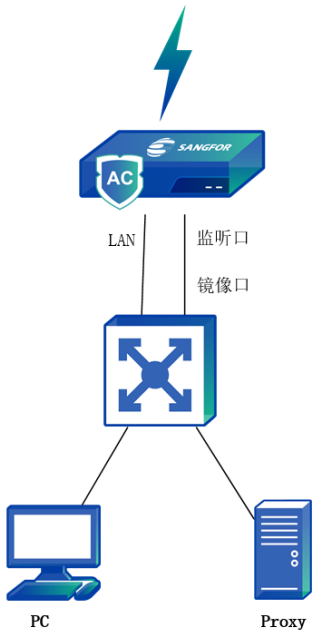
步骤6.PC登录Proxy服务器，登录成功后即可上网。

说明：

1. 若Proxy服务器为ISA服务器，并且ISA服务器采用“windows集成身份认证”方式，则需要勾选[兼容kerberos认证方式]以完成单点登录，并且该方式仅适用于登录数据包穿过AC设备的情况，不适用于镜像方式，同时旁路模式下也不支持该功能。

2. 这种场景下如果[认证策略/认证后处理/高级选项]中勾选了[显示免责声明]，则需要配置从DMZ口做重定向，否则将无法通过认证上网。

第二种情况：Proxy服务器在内网方向，如图所示。



数据流过程如下：

1. 用户通过Proxy服务器代理上网，认证数据不经过AC转发；

2. 在交换机上设置镜像口，把PC到Proxy服务器的数据镜像到AC上；

3. PC成功经过Proxy服务器认证的同时也经过设备的认证。

操作步骤

步骤1.设置认证策略，根据需要使用单点登录的用户的IP或MAC设置认证策略，进入[接入管理/接入认证/PORTAL认证/认证策略/新增认证策略]进行配置。

步骤2.点击进入[接入管理/接入认证/PORTAL认证/单点登录/Proxy]页面进行配置。

步骤3.勾选启用Proxy单点登录，勾选监听计算机登录Proxy的数据，获取登录信息。

步骤4.在Proxy代理服务器地址列表中输入Proxy服务器的IP和监听端口，如果有多个Proxy服务器，则一行一个IP和端口，此处的端口设置Proxy认证的端口即可，如下图所示。

步骤5.如果登录数据不经过设备，需要通过设置镜像口，并将镜像口连接到转发登录数据的交换机镜像口上，点击<其他选项>，设置设备的镜像口。镜像口需要设置空闲网口，已经在使用的网口请不要设置成镜像网口。

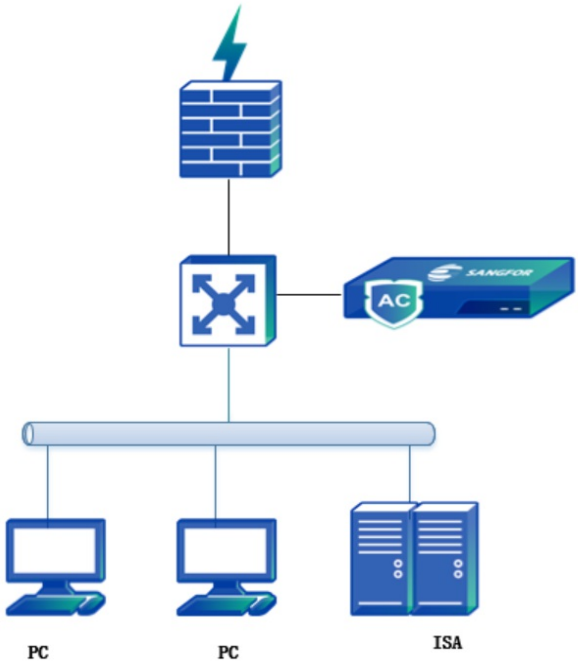
步骤6.PC登录Proxy服务器，登录成功后即可上网。

说明：

当登录数据不经过AC，采用镜像数据的监听方式不支持[兼容Kerberos认证方式]。

使用ISA控件方式

ISA控件方式可用于ISA服务器在内网，登录ISA的数据不经过设备的情况下，通过在ISA服务器上注册扩展插件，将PC登录ISA成功后的信息通过扩展的插件通知设备，来完成用户在设备上的登录。



数据流的过程大致如下：

1. PC通过HTTP代理，通过ISA的PRXOY认证；

2. ISA将PC登录成功的信息发给AC设备；

3. AC设备自动将PC认证通过，放行PC上网数据。

操作步骤

步骤1.根据需要使用单点登录的用户IP或MAC设置认证策略，点击[接入管理/接入认证/PORTAL认证/认证策略]，新增认证策略进行配置。

步骤2.点击进入[接入管理/接入认证/PORTAL认证/单点登录/Proxy]页面进行配置。

步骤3.勾选[启用Proxy单点登录]，勾选[通过Proxy执行指定的登录控件，获取登录信息]，表示使用ISA控件方式实现单点登录。在请输入共享密钥：输入共享密钥。

步骤4.在设备上下载ISA单点登录控件及示例，配置ISA服务器，注册插件并配置SangforAC.ini。

1. 插件MyAuthFilter.dll 放到ISA 安装目录下，如C:/Program Files/ISA server/

2. 运行 regsvr32 “C:/Program Files/ISA server/MyAuthFilter.dll” 注册插件

3. 将示例配置文件SangforAC.ini 放到C 盘根目录下。下面是配置文件的说明：

• ACIP=192.168.0.1 设备IP的地址。

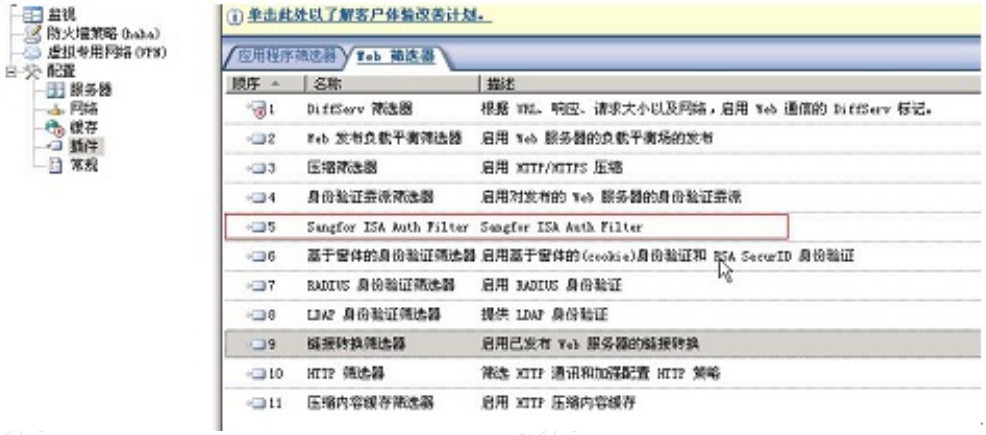
• key=123 登录ISA的数据包加密密钥，要跟设备上设置的一致。

• cycle=30 每个IP 地址发送登录数据包的最小间隔（单位：秒），作用是避免每个IP 地址每发起一个新会话访问一个新网站，就发一次登录数据包，这样发送过于频繁。

• logpath=调试日志路径，为空表示关掉日志，填写路径表示开启日志，默认关掉，请在有需要的时候再打开。另外，请保证NETWORK SERVICE用户对该文件所在目录具有可读写权限。

• maxlogsize=1调试日志文件最大容量（单位：MB），日志文件到达上限值时，会自动清空。charset=UTF-8支持编码有UTF-8、UTF-16、GB2312、GB18030、BIG5。

4. 在ISA 插件面板确认“Sangfor ISA Auth Filter”插件已启用。



步骤5.PC登录Proxy服务器，登录成功后即可上网。

说明

：

1．每次修改SangforAC.ini文件后需要重新注册插件。

2．ISA 插件无法实现当域用户注销或关闭电脑时，让域用户自动从设备上注销。但可以通过在设备控制台上设置超时时间，让用户从设备上自动注销掉。

3．AC和ISA服务器密钥必须一致，且此密钥不要跟其他方式单点登录密钥相同。

4．ISA服务器要放通自身连接AC设备UDP 1773 端口的数据。

5．如果Proxy服务器在AC WAN区域，则需要放通用户认证前访问Proxy服务器的权限。

6．放通权限在[认证策略/认证后处理/高级选项]中，勾选[认证前使用此组权限]，并设置一个组。在这个用户组的上网权限设置中放通Proxy服务器的IP和端口。

6.2.1.3.4.**POP3**

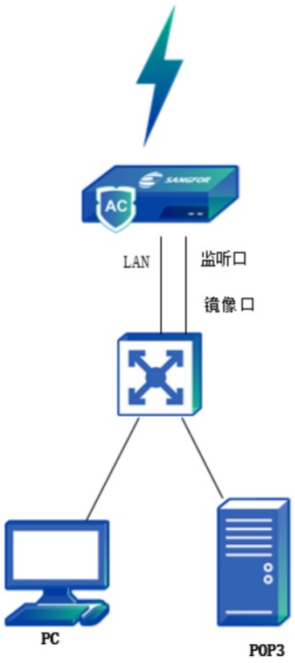
如果用户网络环境中已经部署POP3邮件服务器，并且内网用户登录邮件服务器都有各自的账号和密码，那么可以采用POP3单点登录的方式，内网用户通过POP3服务器的验证之后就通过设备的认证上网。

• 启用POP3单点登录：**开启和关闭POP3单点登录功能。**

• 邮件服务器地址列表：**填写邮件服务器的IP地址。**

用户网络中有邮件服务器，用户信息存放在POP3服务器上，在上网之前，用户使用Outlook、Foxmail之类的客户端登录POP3服务器收发一次邮件，设备通过监听模式监听到用户登录的信息，则设备会自动识别并认证通过，此时用户可以直接上网，而不需要再次输入用户名密码。同时适用POP3服务器在内网和外网情况。下面分两种情况讲述POP3单点登录的设置。

第一种情况：POP3服务器在内网



数据流过程如下：

1. 用户通过邮件客户端和POP3服务器通讯，设备监听整个通信过程。

2. 邮件客户端成功登录POP3服务器的同时，设备自动认证用户，上网不需要再次需入密码。

3. 由于数据交互是在内网，内网登录POP3服务器的数据不经过设备，需要在设备上设置监听口。

操作步骤

步骤1.根据需要使用单点登录的用户IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略]，点击新增认证策略进行配置。

步骤2.点击进入[接入管理/接入认证/PORTAL认证/单点登录/POP3]页面进行配置。

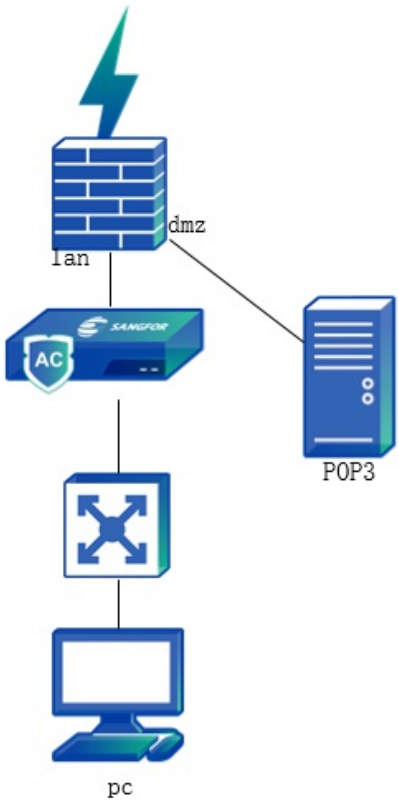
步骤3.勾选[启用POP3单点登录]。

步骤4.在[邮件服务器地址列表]中输入POP3服务器的IP和监听端口，如果有多个POP3服务器，则一行一个IP和端口，此处的端口设置POP3认证的端口（默认是TCP110），如下图所示。

步骤5.此例中登录数据不经过设备，需要通过设置镜像口，并将镜像口连接到转发登录数据的交换机镜像口上，点击<其它选项>，设置设备的镜像口。镜像口需要设置空闲网口，已经在使用的网口请不要设置成镜像网口。

步骤6.PC通过邮件客户端接收一次邮件，登录POP3成功后即可上网。

第二种情况：POP3服务器在外网：



数据流过程如下：

1. PC登录POP3服务器是穿透设备。
2. 设备的内网接口同时作为监听口，无需再设置监听口。

操作步骤

步骤1.根据需要使用单点登录用户的IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略]新增认证策略。

步骤2.点击进入[接入管理/接入认证/PORTAL认证/单点登录/POP3]页面进行配置。

步骤3.勾选[启用POP3单点登录]，在[邮件服务器地址列表]中输入POP3服务器的IP和监听端口，如果有多个POP3服务器，则一行一个IP和端口，此处的端口设置POP3认证的端口（默认是TCP110），如下图所示。

步骤4.PC通过邮件客户端收发一次邮件，登录POP3成功后即可上网。

说明：

1．如果POP3服务器在AC WAN区域，则需要放通用户认证前访问POP3服务器的权限。

2．放通权限在[认证策略/认证后处理/高级选项]，勾选[认证前使用此组权限]，设置一个组。

3．在这个用户组的上网权限设置中放通POP3服务器的IP和端口。

6.2.1.3.5.Web

如果用户网络环境中已经部署WEB服务器，并且内网用户登录WEB服务器都有各自的账号和密码，那么可以采用WEB单点登录的方式，在内网用户通过WEB服务器的验证之后就通过设备的认证上网。配置界面如下图所示。

启用Web单点登录：开启和关闭Web单点登录的开关。

Web认证服务器：设置Web服务器的IP地址。

类型：可以选择Cookie值、POST提交的表单、URL请求中的参数，三种方式适用于不同的web认证服务器。

• Cookie值：**用户认证成功后，web服务器返回一个Cookie值可以通过这个Cookie值判断是否成功登录。**

• Cookie名：**填写认证成功后，服务器返回的Cookie名。**

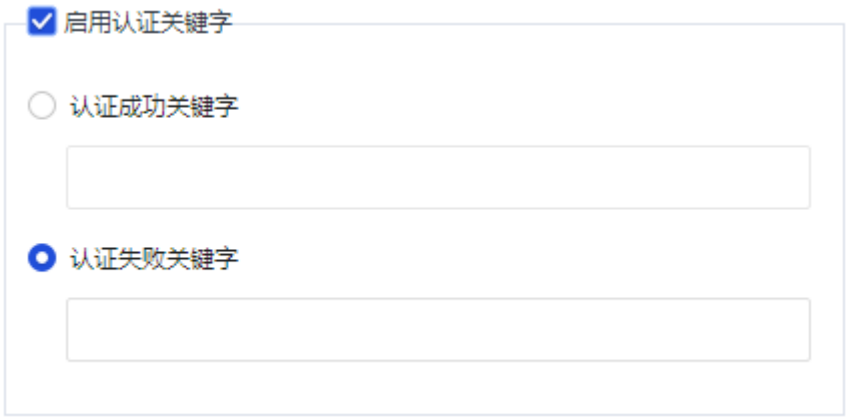
• POST提交的表单：**Web认证时通过POST方式提交用户名时，需要使用这种类型。**

用户表单名称：填写Web认证时，向服务器提交用户名表单名称，支持正则表达式。

支持启用/禁用认证关键字；禁用则表示认证时无需校验关键字。

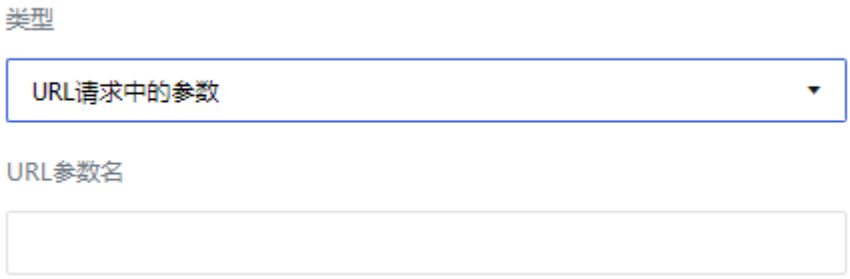
认证成功关键字：用来识别Web登录是否成功的关键字。返回结果中，如果包含了设定的关键字，则判断为Web单点登录成功。

认证失败关键字：回结果中，如果包含设定的关键字，则判断为Web单点登录失败。



URL请求中的参数：当Web认证是通过http get请求提交认证信息时引用。

URL参数名：填写URL请求中认证字段对应的参数名。



指定表单编码类型：如果出现乱码，则可尝试指定编码类型，否则无需设定，设备会自动识别选用的编码类型。

场景案例

Web单点登录一般适用于客户有自己的Web服务器，且账号信息均保存在Web服务器上，客户想要实现内网用户上网前通过自己Web服务器的认证同时也通过AC设备的认证。Web服务器在内外网都支持。

全网行为管理支持从POST值、Cookie值和URL参数中提取登录Web服务器的用户名，具体选择哪种方式取决于用户登录Web服务器时提交用户名所用的方式。

当用户使用POST提交用户名登录Web服务器时，Web服务器会依据登录成功或者失败的结果返回对应的值，所以可以根据Web服务器的返回值（关键字）来确定用户是否登录成功，从而决定该用户是否在AC上线。

通过Cookie和URL这两种方式提交用户名时，Web服务器不会有回应，所以无法判断是否登录成功，只能实现抓取到用户名就立即上线。

本次示例均为POST的方式提交用户名。

场景一：Web服务器在AC设备的LAN口区域，且用户访问Web服务器的流量不会经过AC设备。

操作步骤

步骤1.在[接入管理/接入认证/PORTAL认证/单点登录]界面启用Web单点登录。

在[Web认证服务器]栏填写Web服务器的域名或者IP地址。

类型：选择“POST提交的表单”。

用户表单名称：是用户登录Web服务器时提交的用户名所对应的表单。

启用认证关键字：是为了判断该用户提交用户名和密码后是否成功登录了Web服务器，从而决定该用户是否在AC上线。

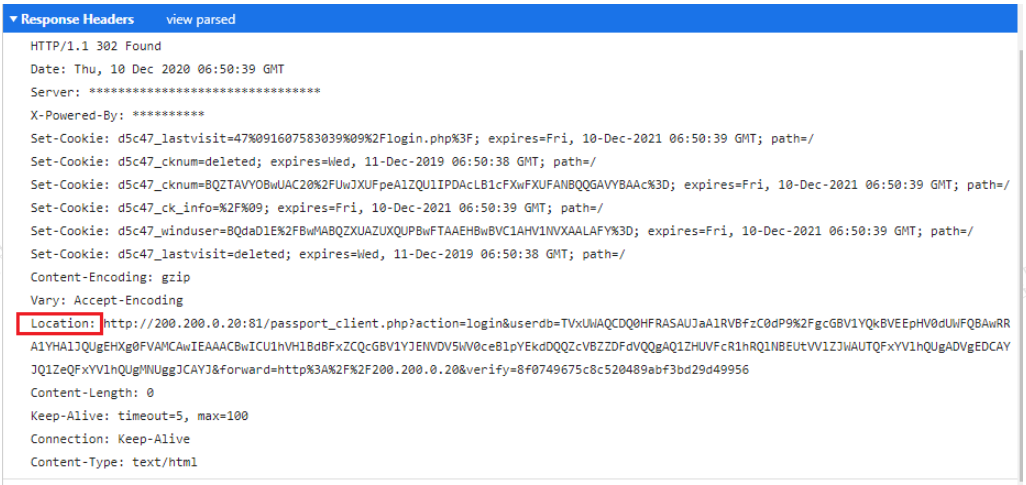
表单名和认证关键字均需要依据实际情况填写，如果不清楚可通过抓包获取该信息。

步骤2.确认表单名和认证关键字。使用抓包工具抓取用户登录Web服务器的交互过程从而确认表单名和关键。如下图所示：

通过抓包工具抓取用户登录Web服务器的数据包，在POST表单里可以看到提交用户名的表单名为：pwuser

通过比对登录失败和登录成功的数据包，能够发现登录成功的POST返回值里面携带了Location，获取认证失败关键词同理。

登录成功返回值



登录失败返回值

步骤3.在[单点登录/其他选项]界面勾选[启用镜像网口]并选择对应的镜像网口名，然后点击<提交>保存配置。在本场景下用户登录的Web服务器在内网且流量不会经过AC，所以需要通过镜像流量来监听用户登录Web服务器的数据包从而获取用户名等信息。

步骤4. 在[接入管理/接入认证/PORTAL认证]新增认证策略。[认证方式]选取单点登录，在[认证范围]根据需求配置进行单点登录的认证范围。

步骤5.用户成功登录Web服务器，同时在 AC上线获取对应的外网访问权限。

场景二：Web服务器在AC设备的WAN口区域，当用户访问Web服务器的流量经过AC设备。

步骤1.配置用户认证前网络访问权限。因为Web服务器在AC的WAN口区域，所以用户在完成认证上线前需要能够访问Web服务器，否则无法完成认证。

步骤2. 通过配置[认证前使用此组权限]的功能可以使用户在未认证前能够访问有限的网络资源。目前只有密码认证（包括单点登录失败后匹配密码认证）的认证策略支持设置“认证前使用此组权限”的功能。

步骤3.在[接入管理/本地组用户]点击<新增>添加一个用户组，以该组的身份配置用户认证前的需要访问的网络权限。当用户认证失败就会匹配此用户组的访问访问权限。

步骤4.自定义URL或者自定义应用。在某些场景下需要开放企业内部私有的应用或者URL，此时则需要在AC上自定义企业内部的一些应用或者URL。此处以自定义应用为例：在[系统管理/对象定义/自定义应用]界面点击<新增>按钮，配置应用相关参数。

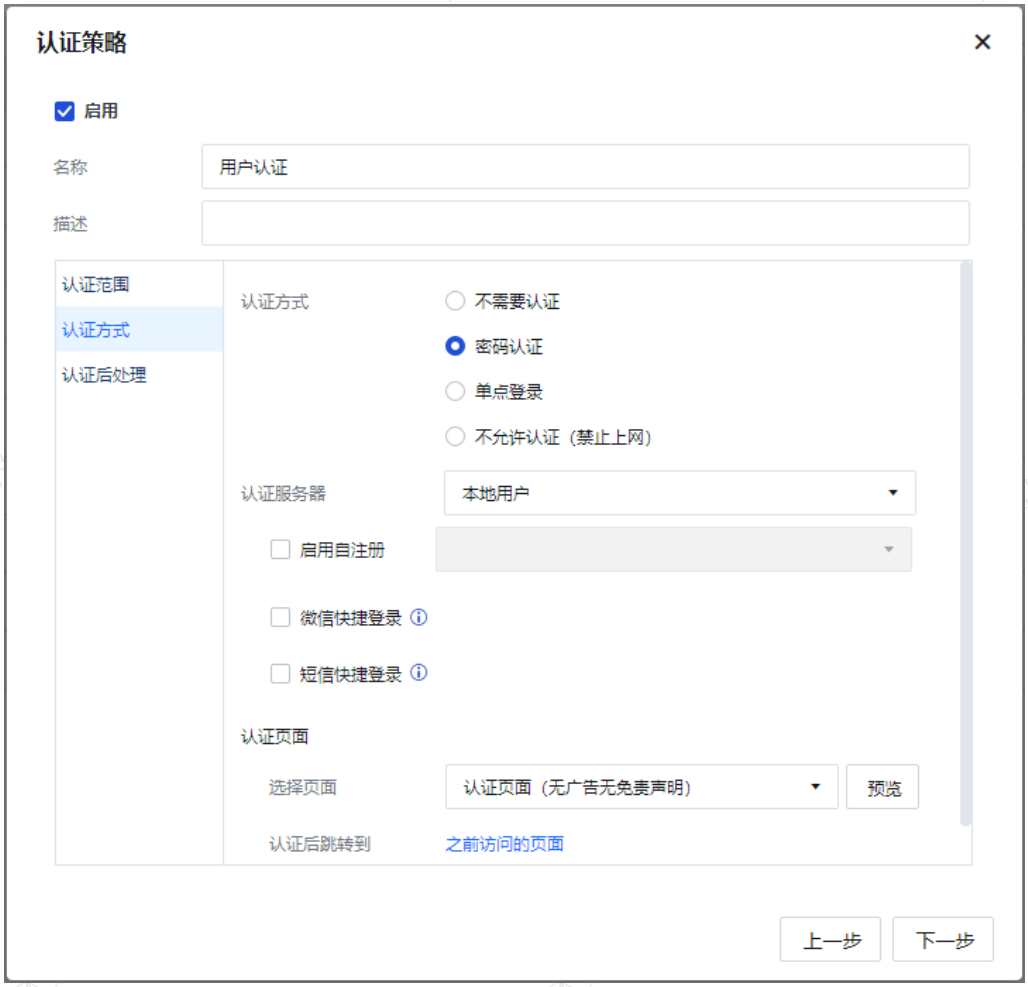
步骤5.在[行为管理/访问权限策略]界面点击<新增>按钮，添加[访问权限策略]用于配置认证前的网络访问权限。

步骤6.勾选[应用控制]，并在应用控制栏内先添加一条拒绝所以的策略，然后再添加一条放通策略。该放通策略用于放通认证前需要访问的应用，比如步骤2自定义的内网应用。

在[适用对象]页面勾选认证前的组对象，最后点击<提交>即可。

步骤7.配置认证策略。在[接入管理/接入认证/PORTAL认证]界面点击<新增>按钮配置密码认证策略，并根据实际需求配置认证策略适用范围。如“10.68.10.3/24”。

步骤8.在[认证方式]栏选择密码认证。（如果认证方式为“单点登录”但配置了失败后匹配密码认证，也支持设置“认证前使用此组权限”的功能）



步骤9.启用[认证前使用此组权限]。在认证后处理栏点击<高级选项>，然后勾选[认证前适用此组权限]并配置好相应的组名。配置如下图所示。

步骤10.在[接入管理/接入认证/PORTAL认证/单点登录]界面启用Web单点登录。

• Web认证服务器：**填写Web服务器的域名或者IP地址；**

• 类型：**选择“POST提交的表单”。**

• 用户表单名称：**是用户登录Web服务器时提交的用户名所对应的表单。**

• 启用认证关键字：**是为了判断该用户提交用户名和密码后是否成功登录了Web服务器，从而决定该用户是否在AC上线。**

• **表单名和认证关键字均需要依据实际情况填写，也可通过抓包获取该信息。**

步骤11.确认表单名和认证关键字。使用抓包工具抓取用户登录Web服务器的交互过程从而确认表单名和关键。

通过抓包工具抓取用户登录Web服务器的数据包，在POST表单里可以看到提交用户名的表单名为：pwuser。

通过比对登录失败和登录成功的数据包，能够发现登录成功的POST返回值里携带了Location，获取认证失败关键词同理。登录成功返回值和登录失败返回值请参靠案例一的图。

步骤12.在[接入管理/接入认证/PORTAL认证]界面为需要进行单点登录的用户配置认证策略。[认证方式]选取单点登录，在[认证范围]根据需求配置进行单点登录的认证范围。

说明

：

需要配置“单点登录的用户失败后匹配密码认证”，否则[认证前使用此组权限]的功能不会生效，导致无法访问Web服务器。

步骤13.用户成功登录Web服务器，同时在 AC上线获取对应的外网访问权限。

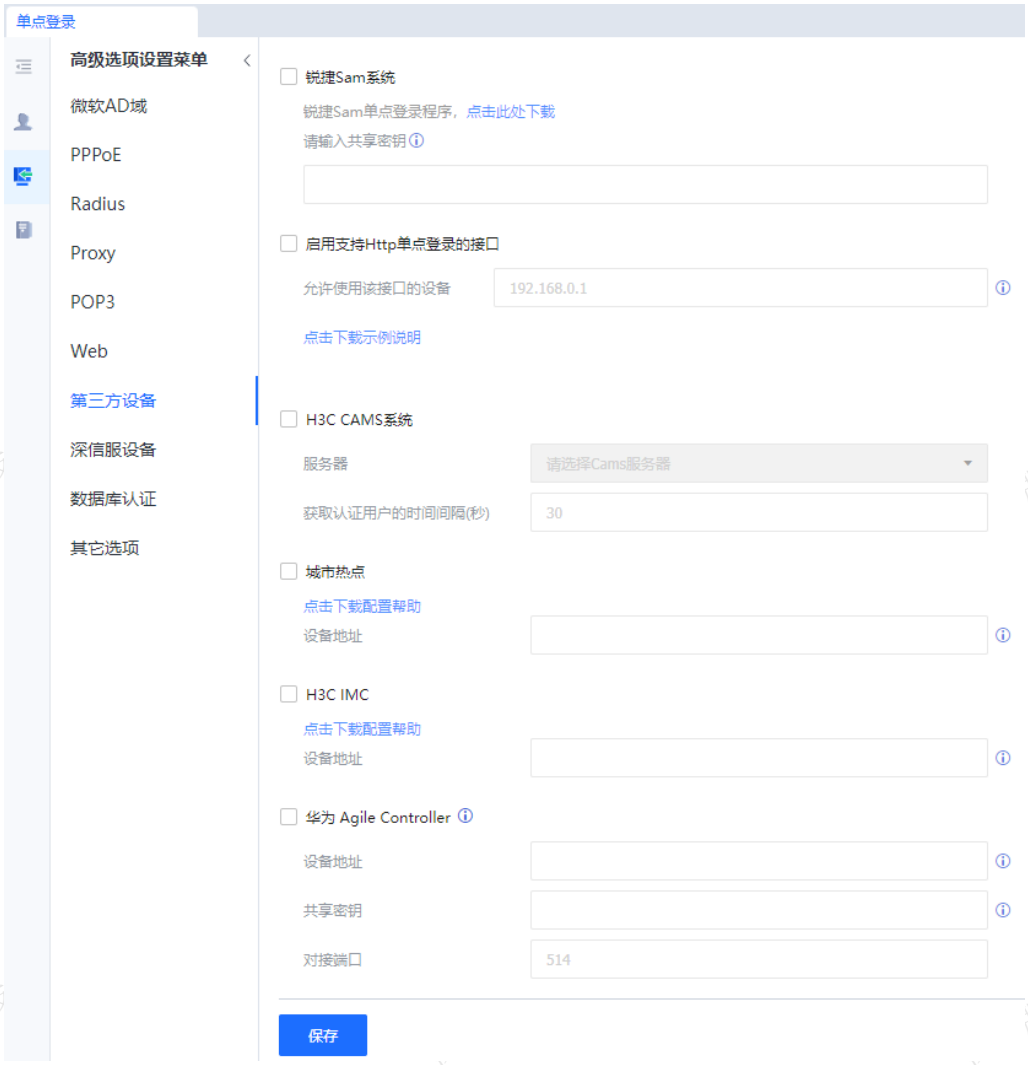
说明

：

截止到本文发布为止，Web单点登录暂时不支持https的Web应用登录。

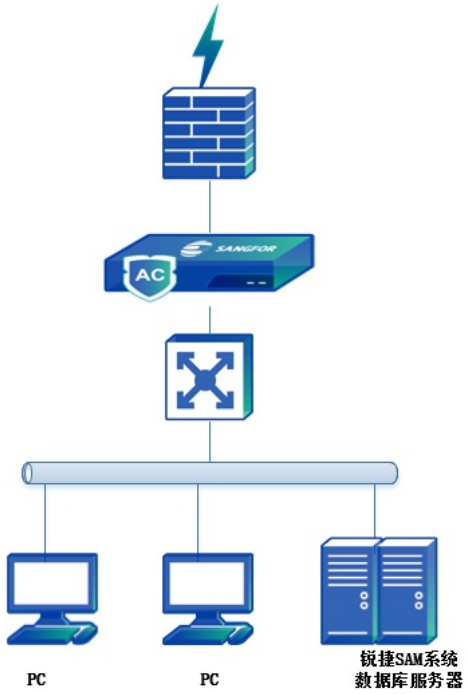
6.2.1.3.6.第三方设备

某些网络环境中已经存在其他的第三方认证系统作为用户认证和组织结构的管理，此时设备能够跟这些第三方的认证系统结合使用，做单点登录。目前设备支持的其他第三方厂商的认证系统有锐捷Sam系统、HTTP单点登录接口、H3C CAMS系统、城市热点、H3C IMC系统和华为Agile Controller。



锐捷Sam系统结合认证

锐捷Sam系统是一套宽带上网认证计费管理系统，常用于高校及二级运营商用户，用户上网前必须通过锐捷Sam系统的身份认证，用户通过Sam系统的认证/注销后，自动在AC上完成认证/注销。如图所示。



数据流的过程如下：

1. PC通过锐捷Sam系统认证服务器的认证/注销。

2. 锐捷Sam系统数据库服务器通知AC设备认证/注销用户，实现单点登录和注销。

操作步骤

步骤1.设置认证策略，根据需要使用单点登录的用户的IP或MAC设置认证策略，点击[接入管理/接入认证/PORTAL认证/认证策略]新增单点登录认证方式的认证策略。

步骤2.点击进入[接入管理/接入认证/PORTAL认证/单点登录/第三方设备]页面进行配置。

步骤3.启用锐捷Sam系统并设置共享密钥。

步骤4.在设备上下载锐捷Sam单点登录程序，在Sam系统的数据库服务器上配置，使得pc登录到Sam系统时，数据库服务器向AC发送用户认证信息。

以锐捷Sam系统数据库为Sql Server2005为例，说明锐捷Sam系统数据库服务器需要做的设置：

1. 在[接入管理/接入认证/PORTAL认证/单点登录/第三方设备/锐捷Sam系统]下载rjsam.zip（内含logon.exe和触发

器sql脚本)到服务器上。解压后，得到如下内容。

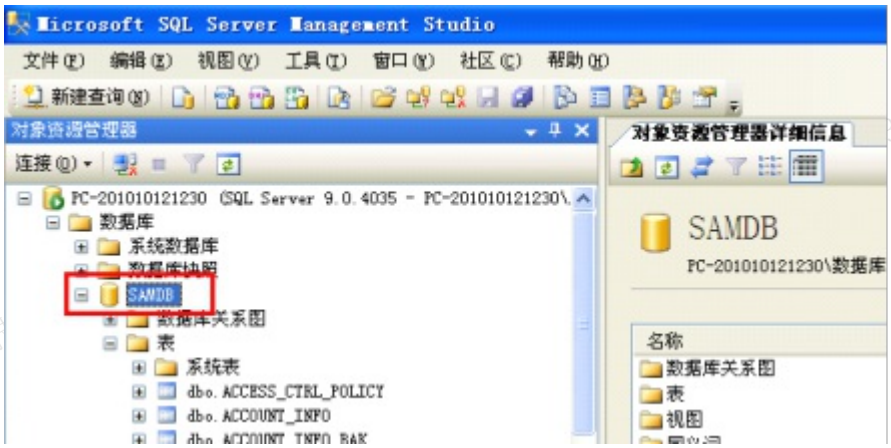
2. 将触发器所需调用的应用程序logon.exe 拷到SAM 服务器对应目录下。

3. 文件夹2005中存放了为sql server 2005定制的触发器sql语句，以logon_trigger.sql为例，打开此文件，将内容全选复制后，粘贴到sql server 查询管理器中，根据实际情况修改如下配置（logout_trigger.sql和update_trigger.sql的修改同logon_trigger.sql）：

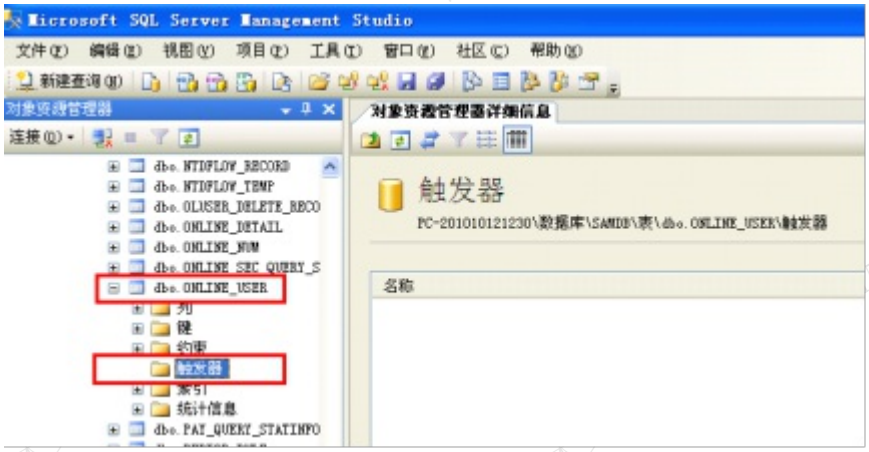
```
set @i = 1
--logon与authd通信的共享密钥
set @sharekey = '123'
--ac 设备的ip地址
set @acip = '200.200.65.145'
--可执行文件路径要改成logon.exe放置绝对路径,路径中不要含有空格和`~!@#$%^&*()?等特殊字符
set @progpath = 'c:\logon'
--用户名的本地字符编码 可选项有gb18030,gb2312,big5,utf-8,utf-16
set @localcodepage = 'utf-8'
```

4. 由于上述3个触发器都调用了master 数据库的xp_cmdshell 命令，该命令默认被SQL SERVER 2005 禁止调用。这需要执行下图的xp_cmdshell.sql 来解除禁用。在[Sql Server 2005 Management Studio] 中打开该文件，按[执行]按钮执行。

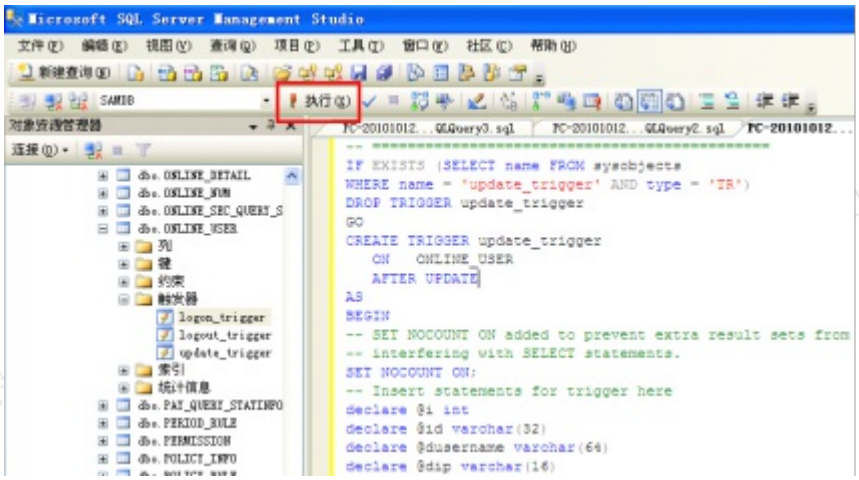
5. 打开Sql Server 2005 Management Studio，找到SAMDB 数据库。



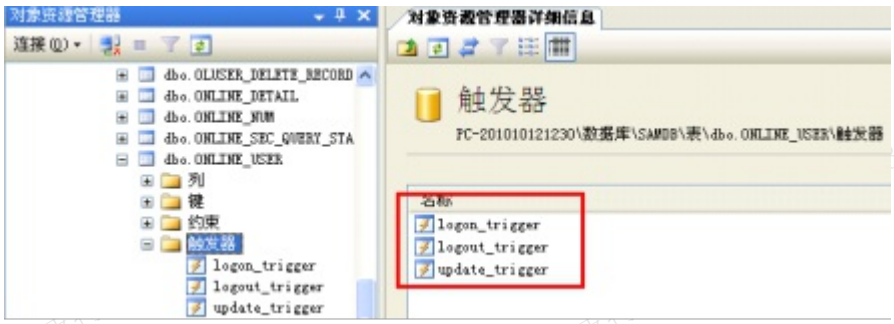
6. 找到[ONLINE_USER]表，点击触发器文件夹图标，右边[对象资源管理器详细信息]空白区域没有任何条目，没有新建任何针对“ONLINE_USER”表的触发器。



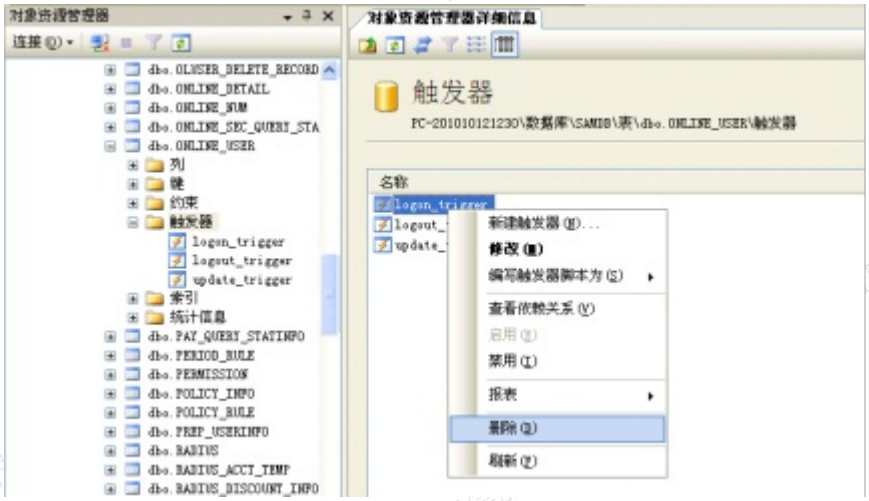
7. 打开文件夹2005目录，双击步骤3描述的三个文件，它们被打开在“Sql Server 2005 Management Studio ”中，点击工具条上的<执行>按钮，当前激活tab 页对应的触发器被安装，切换tab 页，对另外两个触发器也执行同样的安装操作。

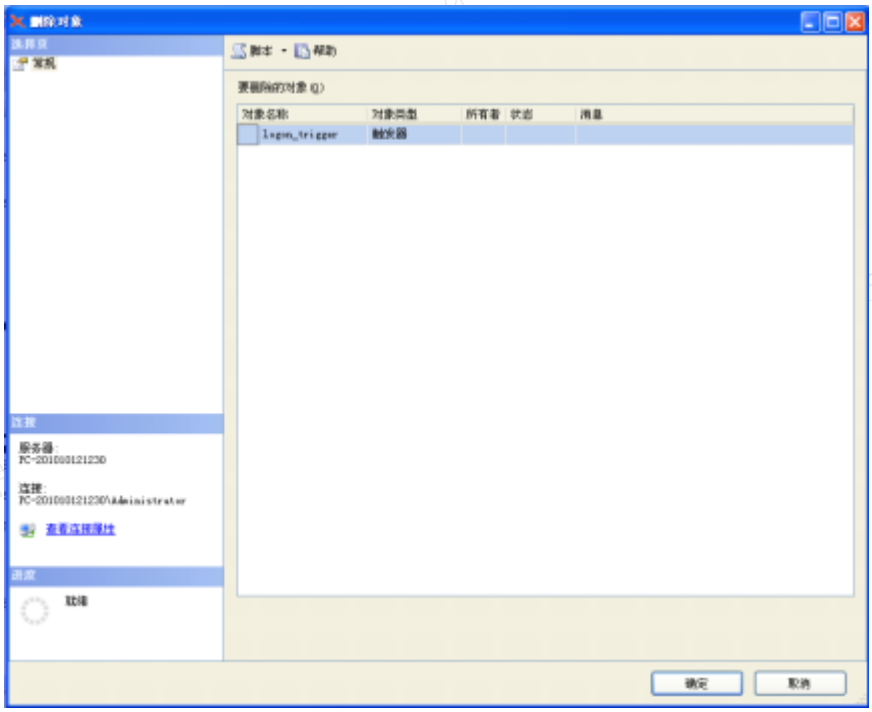


8. 切换到“对象资源管理器详细信息”tab 页，刷新空白区域，可看到触发器完成安装。



9. 如果需要删除触发器，则在[Sql Server 2005 Management Studio]的[对象资源管理器详细信息]中点击对应触发器，可以看到弹出菜单中有删除项，点击该项将弹出删除对象对话框，点击该对话框的确定键，即可删除对应触发器。





步骤5.用户通过锐捷SAM认证的同时通过设备的认证上网。

1. 触发器在Sql Server2000 锐捷服务器上的安装过程与2005 版类似，不同的是要选择在2000 目录下的触发器安装，若存储过程xp_cmdshell已启用，则不需要执行xp_cmdshell.sql。
2. 若锐捷sam系统数据库名不是samdb，则将触发器sql语句第一行 use SAMDB的[SAMDB]修改成实际的数据库名，若表名和字段名跟示例不同，也需要酌情修改。
3. 注意trigger语句中的如下字段，如果多个用户可能同时登录或注销，需要根据用户机构上网人数将@i允许的值改大，一般建议修改最大不要超过2000（高端设备最多支持3000），若保持默认不修改，则用户环境若有两个用户同时登录，则AC只认证一个用户，导致另外一个用户无法上网。

```
--如果数据库一次可以删除多个用户，将下面@i>0的条件改一下，如改成@i>9,可以一次最多触发程序执行10次
--如果注释掉下面两行则一次可以触发的程序执行次数不受限制，但在这些情况下需要考虑太多程序并发运行的风险
IF @i>0 BREAK
SET @i = @i + 1
```

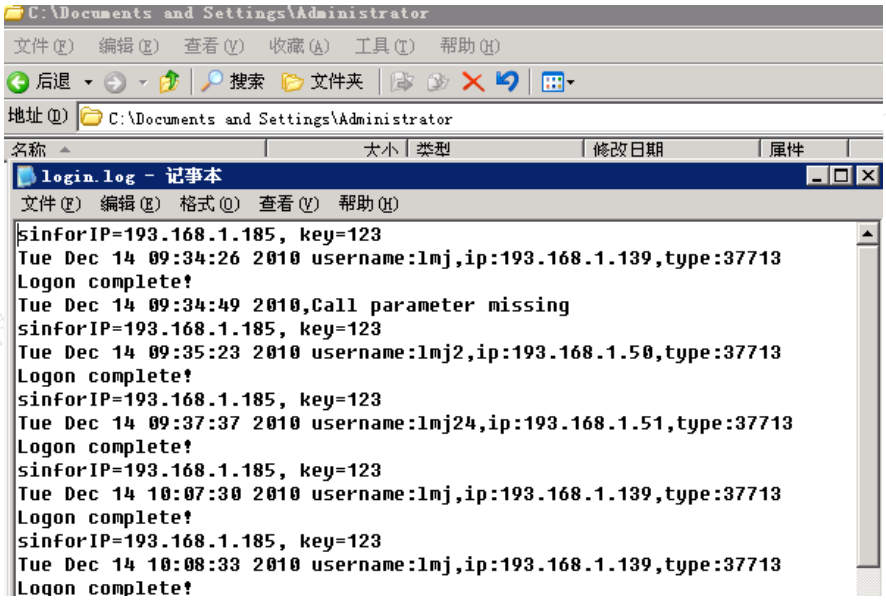
4. 如下，修改成可以支持最多10个用户同时登录或者注销。

```
IF @i>9 BREAK
SET @i = @i + 1
```

5. 注意trigger语句中的如下字段，当logon.exe向AC发送认证信息时，为保护服务器性能，默认是不开启日志的，如果需要开启日志，则将上一段置换如下，即带-l参数表示启用日志。

```
set @cmd = @progpath + ' -o ' + @ip + ' "' + @username + '" "' + @sharekey +'" ' + @localcodepage + ' '+@acip
--如果要启用日志请注释掉上面一行，开启下面的一行
--set @cmd = @progpath + ' -o ' +  @ip + ' "' + @username + '" "' + @sharekey +'" ' + @localcodepage + ' ' +@acip + ' -l'
```

6. 这样在数据库服务器用户主目录下会产生日志如下。



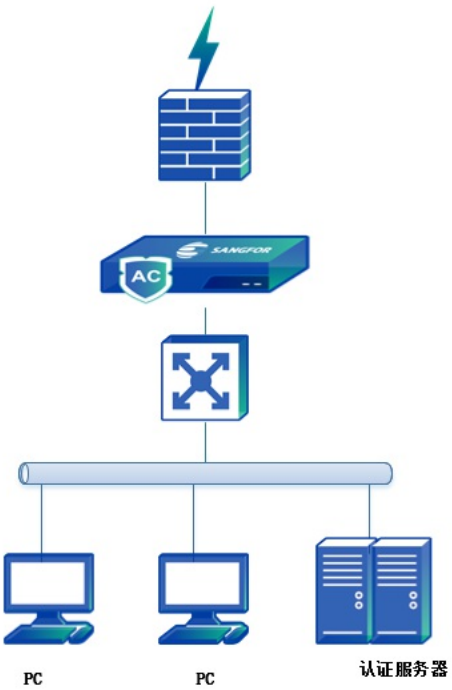
7. 设备和trigger脚本中配置的密钥一致，且此密钥不要与其他方式单点登录密钥相同。

8. 要求设备和锐捷Sam服务器能互相通讯，锐捷SAM服务器连接设备UDP：1773端口发送认证信息，不要求用户登录Sam系统的数据经过设备。

9. 此方法不限于锐捷SAM系统，适用于所有后台数据库为MS SQL SERVER 2000/2005的数据库系统，需要酌情修改SQL脚本，使得相关库名 、表名、字段名与实际使用环境匹配。

支持HTTP单点登录的接口结合认证

设备提供的HTTP 单点登录接口，可以向任何第三方认证设备，提供基于HTTP(S)协议，GET 方法的单点登录/注销功能。



数据流的过程如下：

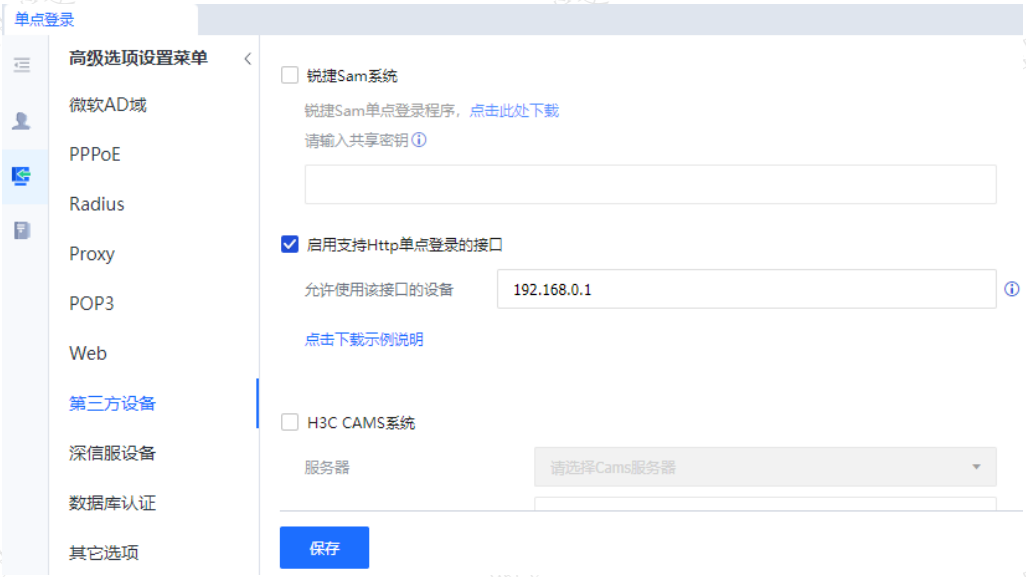
1. PC通过http/https方式访问认证服务器，并通过认证服务器的认证/注销。
2. 认证服务器认证/注销页面做处理，使得能通知AC设备上线/注销对应用户，完成单点登录。PC通过AC认证，正常上网。

操作步骤

步骤1.根据需要使用单点登录的用户IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略]新增认证策略。

步骤2.在[接入管理/接入认证/PORTAL认证/单点登录/第三方设备]进行单点登录配置。

步骤3.勾选[启用支持HTTP单点登录的接口]，设置允许使用该接口的设备IP。



步骤4.点击下载示例说明，其中包含了Logon.js和Logon.html，修改Logon.html，并配置提供认证的服务器。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<title> HTTP单点登录接口示例</title>
<script src="ACLogon.js" type="text/javascript"></script>  ←这里必须要 →
</head>

<body>
    <form>
        ip:<input type=text id='ip' ></input><br/>
        usr:<input type=text id='usr'></input><br/>
        grp:<input type=text id='grp'></input><br/>
        <a
href="javascript:sendToAc('200.200.65.145','logon',$('#ip').val(),$('#usr')
.val(),$('#grp').val());"> login<a><br/><-- 这里是登录 -->      <a
href="javascript:sendToAc('200.200.65.145','logout',$('#ip').val(),$('#usr'
).val(),$('#grp').val());"> logout<a><br/><-- 这里是注销 -->
    </form>
 <-- 200.200.65.145是sangfor AC的IP地址,使用该示例还请修改-->
</body>
</html>
```

步骤5.PC通过http/https服务器的认证/注销后自动在设备上通过认证/注销。

说明：

1．http单点登录接口方式，适用于结合城市热点计费管理系统，同时也支持和其他web认证系统结合，需要web服务器做二次开发以配合完成单点登录。

2．不需要此功能时，注意不要勾选“启用支持Http单点登录的接口”。

H3C CAMS系统结合认证

H3C CAMS系统同锐捷sam系统，也是一套宽带上网认证计费管理系统，常用于高校及二级运营商用户，AC设备根据H3C CAMS提供的接口与之完成对接，定时从CAMS系统中获取用户信息，并更新自己的在线用户列表/用户列表，以完成单点登录。

数据流的过程如下：

1. PC通过H3C CAMS系统的认证。
2. 设备定时同步H3C CAMS系统上的组织结构和在线用户。
3. PC以AC设备取到的在线用户的身份上网。

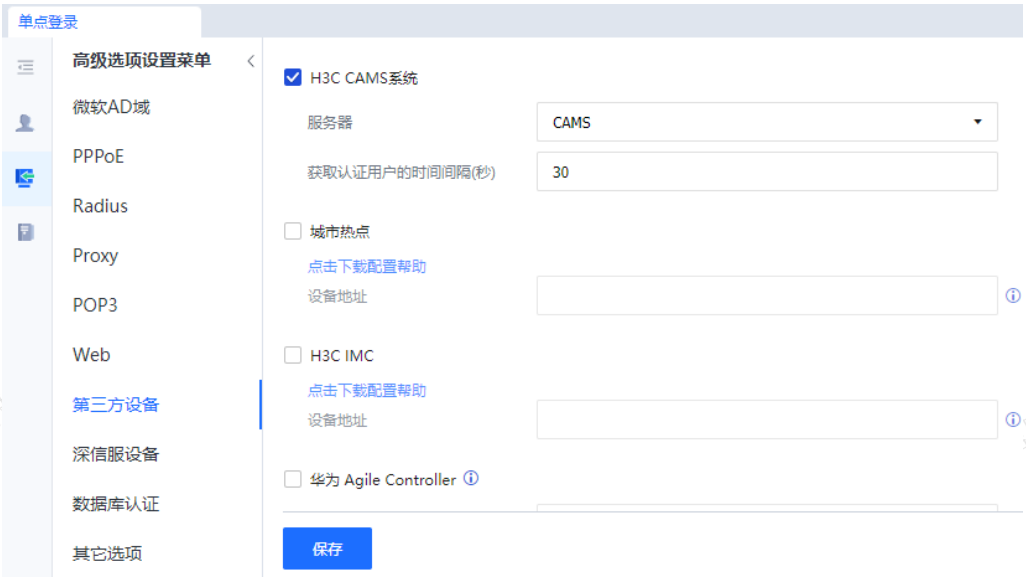
操作步骤

步骤1.根据需要使用单点登录的用户IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略]新增认证策略。

步骤2.设置H3C CAMS 服务器，点击进入[接入管理/接入认证/PORTAL认证/认证服务器]，进行设置（参见第三方设备单点登录）。

步骤3.进入[接入管理/接入认证/PORTAL认证/单点登录/第三方设备]页面进行配置。

步骤4.勾选[H3C CAMS系统]，选择在外部认证服务器中设置的CAMS服务器。



步骤5.用户通过H3C CAMS系统的认证后，即可通过设备上网。

说明

：

1．H3C CAMS支持用户自动同步，具体请参见[用户管理/用户自动同步]。

2．在某些情况下，用户通过认证服务器认证之后在一个时间间隔后（取决于[获取认证用户的时间间隔]设置）才会通过AC的认证，建议认证策略设置单点登录失败时选择[不需要认证]的认证方式。

H3C IMC结合认证

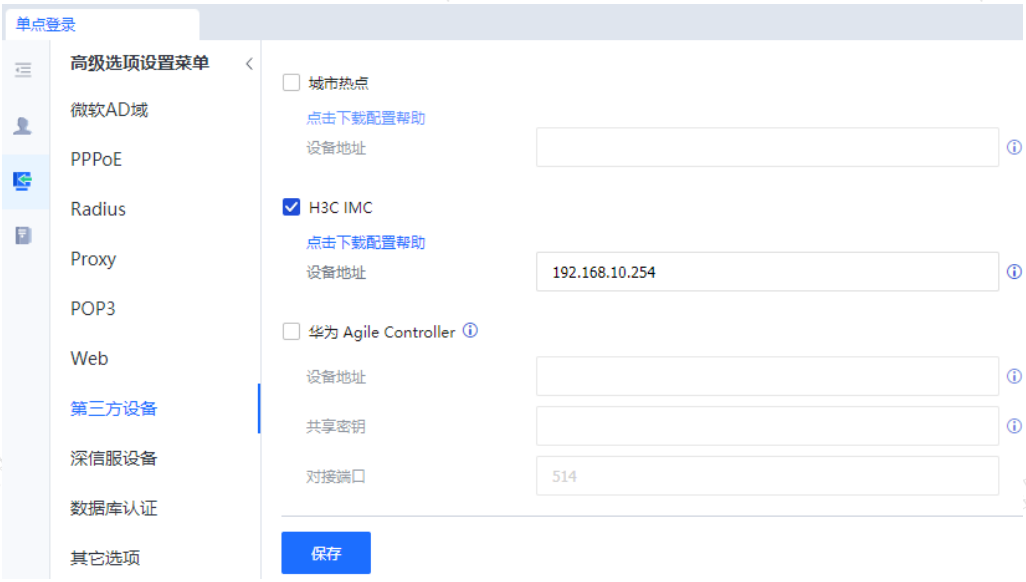
客户环境中已经有了H3C IMC认证服务器，需要实现终端通过H3C IMC认证后不需要再进行AC入网认证，同时在AC上能看到终端以H3C IMC上用户名上线。

数据流的过程如下：

1. 终端通过H3C IMC系统上/下线后，IMC系统会向AC发送报文。
2. AC收到IMC发送的终端上/下线报文后，会解析出上/下线终端的用户名和IP，然后通过单点登录流程实现终端上/下线。

操作步骤

步骤1.配置单点登录。在AC设备[接入管理/接入认证/PORTAL认证/单点登录/第三方设备]选择H3C IMC 并填写H3C IMC服务器地址，点击<提交>，如下图所示。



步骤2.配置认证策略。根据内网的需求设置认证范围，认证方式选择单点认证，单点登录失败选项。可以根据客户需求设置，如下图所示。

步骤3.在H3C IMC系统上配置[用户上下线通知参数配置]，如下图所示。（注意：不同版本的IMC服务器配置界面可能有所不同。）

步骤4.服务器IP地址配置为开启了单点登录的AC设备的IP地址，服务器端口为：61442。共享密钥暂可忽略不计，无影响。

城市热点结合认证

城市热点是一套认证计费管理系统，广泛应用于教育、电信、广电、政府等各个领域，不管城市热点使用的B/S认证还是C/S认证，AC设备都能够与之结合进行用户认证。用户上网前必须通过城市热点系统的身份认证，用户通过城市热点系统的认证/注销后，自动在AC上完成认证/注销。

数据流的过程如下：

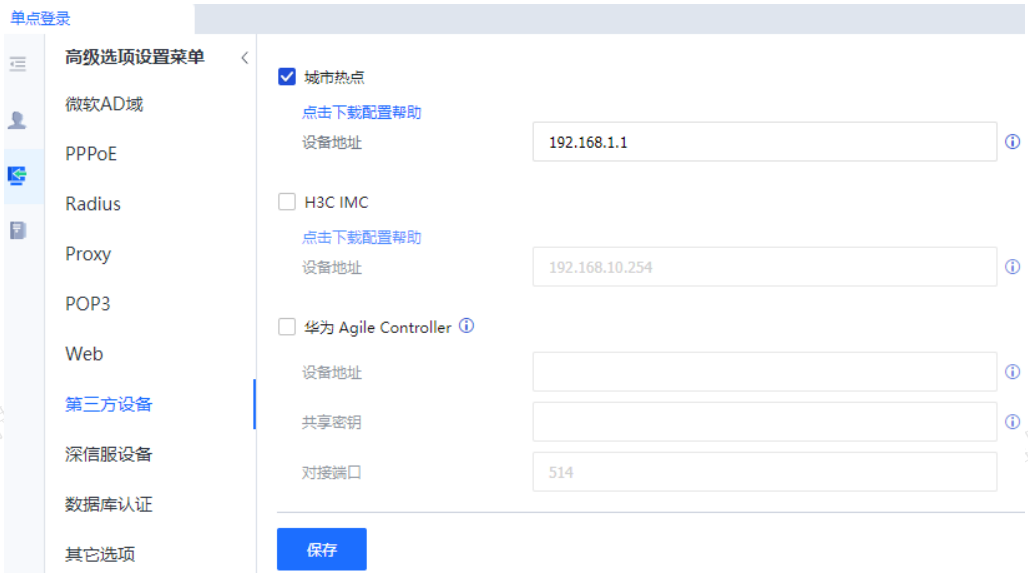
1. PC通过城市热点认证服务器的认证/注销。

2. 城市热点认证服务器通知AC设备认证/注销用户，实现单点登录和注销。

操作步骤

步骤1.根据需要使用单点登录的用户IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略]新增认证策略。

步骤2.在[接入管理/接入认证/PORTAL认证/单点登录/第三方设备] 勾选<城市热点>并设置设备IP地址。



步骤3.配置城市热点系统。有关城市热点的配置请联系相应厂商，此处不再举例。

华为Agile Controller结合认证

华为Agile Controller是一个基于用户与应用的网络资源自动化控制系统，支持准入控制、访客管理、业务随行、业务编排，作为园区网络的集中化控制核心，全局控制园区网络的用户、业务与安全等策略。企业已经部署Agile Controller，并启用准入控制功能（MAC、802.1x、Portal、SACG），实现终端用户通过Agile Controller认证后不需要再进行AC入网认证，同时在AC上能看到终端以Agile Controller上的用户名上线。

数据流的过程如下：

1. 终端通过Agile Controller上/下线后，Agile Controller会向AC发送报文。
2. AC收到Agile Controller发送的终端上/下线报文后，会解析出上/下线终端的用户名、IP、MAC和用户组，然后通过单点登录流程实现终端上/下线。

操作步骤

步骤1.华为Agile Controller已经完成部署，并启用准入控制功能（MAC、802.1x、Portal、SACG）。

步骤2.在华为Agile Controller设备中进入[系统/服务器配置/上网行为管理设备配置]，点击<增加>新建上网行为管理设备，设置联动深信服AC相关参数，配置完成后点击<确定>。

IP地址：深信服AC设备的IP地址。

设备名称：深信服AC设备的名称，用于标识设备，方便管理。

端口：深信服AC设备使用该端口与 Agile Controller 进行联动， 默认端口为8001， 需要与深信服AC 配置

的端口保持一致。

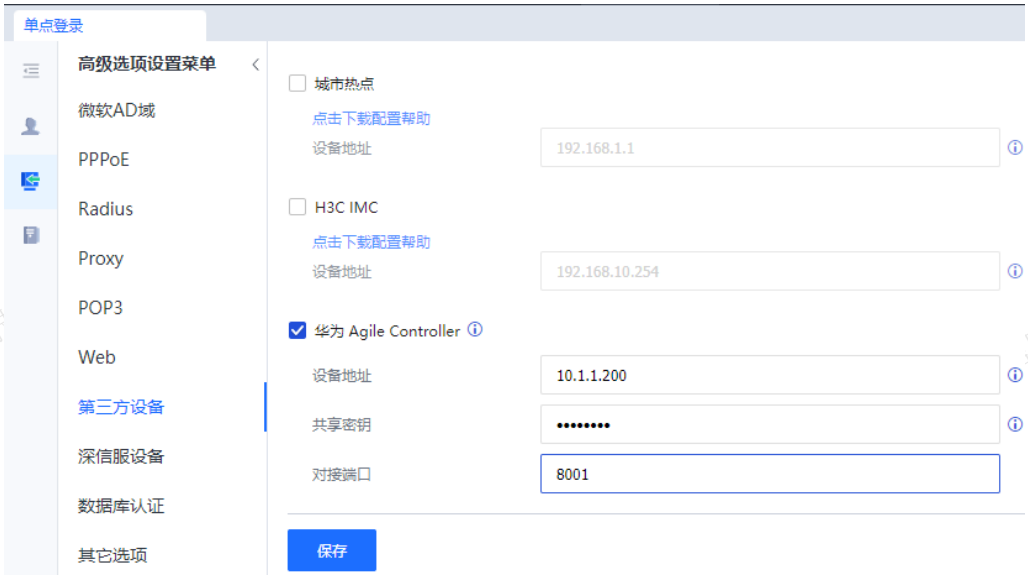
接入密码：与深信服AC设备侧配置的共享密钥保持一致。

加密算法：设置Agile Controller与深信服AC设备之间通信的加密算法。AC 目前只支持AES128加密算法。

终端IPv4地址列表：输入需要单点登录到上网行为管理的终端用户IPv4地址或网段。AgileController只会发送属于该列表的用户登录/注销消息给深信服AC。一个 IP 地址或IP地址段占一行。IP地址段的格式为“IP1-IP2”或“IP/掩码长度”。IP 地址段遵循少而精的原则，因为包含的IP 地址数量越多，AC设备的运行效率会降低。例如，网段192.168.10.1/24中只有192.168.10.1-192.168.10.10 十台终端主机，则不要配置192.168.10.1/24，而配置 192.168.10.1-192.168.10.10。

终端 IPv6 地址列表：启用 IPv6 后，输入需要单点登录到上网行为管理的终端用户 IPv6 地址或网段。Agile Controller 只会发送属于该列表的用户登录/注销消息给深信服AC。一个IP地址或IP地址段占一行。IP 地址段的格式为“IP/掩码长度”。IP 地址段遵循少而精的原则，因为包含的IP地址数量越多，AC设备的运行效率会降低。

步骤3.在深信服AC设备导航栏进入[接入管理/接入认证/PORTAL/单点登录]，选择“第三方设备”，勾选“华为Agile Controller”，配置相关参数后点击<提交>。



设备地址：配置华为Agile Controller设备地址。

共享密钥：与华为Agile Controller设备侧配置的接入密码保持一致。

对接端口：深信服AC设备使用该端口与华为Agile Controller 进行联动，默认端口为514，需要与华为Agile Controller配置的端口保持一致。

步骤4.配置单点登录认证策略。在[接入管理/接入认证/PORTAL/认证策略]新建认证策略，在“认证范围”填入需要单点登录的用户IP地址或网段，在“认证方式”选择单点登录，已开启单点登录方式显示“Agile Controller”，“认证后处理”选择单点登录用户上线的用户组，最后点击<提交>。

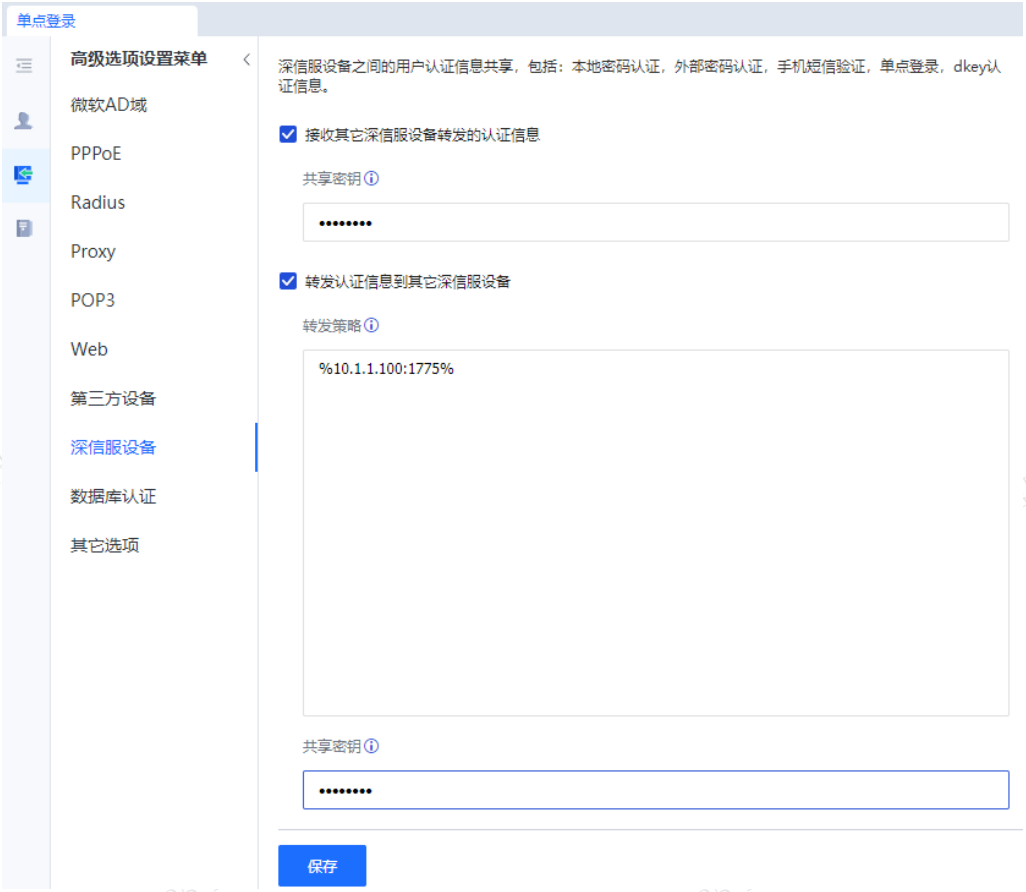
步骤5.用户在华为Agile Controller通过认证后发送上线报文到深信服AC，用户信息同步在深信服AC上线。

6.2.1.3.7.深信服设备

AC设备支持当前在线的用户名和IP地址同步给深信服的其他设备，实现用户同步。

深信服设备之间的用户认证信息共享，包括：本地密码认证，外部密码认证，手机短信验证，单点登录，Dkey认证信息。

AC设备能够和第二台AC/SG设备结合做认证，用户网络环境中部署了两台深信服设备，其中一台设备作认证，另外一台设备作审计控制，只要用户通过了认证设备的认证后，审计控制设备就能够同步认证设备的用户信息，对用户进行审计控制。



勾选[接收其他深信服设备转发的认证信息]：则设备接收其他设备发来的认证信息，并自动添加认证用户，需要设置和转发设备一致的共享密钥。

勾选转发认证信息到其他深信服设备：将本设备的认证信息发给其他设备。

转发策略：用于设置接收认证信息设备策略。

对源IP的控制：%转发IP%，表示转发范围是全部，必须要有两个% 分隔。

书写格式：适用范围%目标设备%策略描述。

适用范围：支持IP和控制器名称，多条件用分号隔开。

目标设备：支持IP或IP：端口。多条件用分号隔开。

共享密钥：于设置发送认证信息时加密的密钥，接收设备和发送设备需要保持一致。

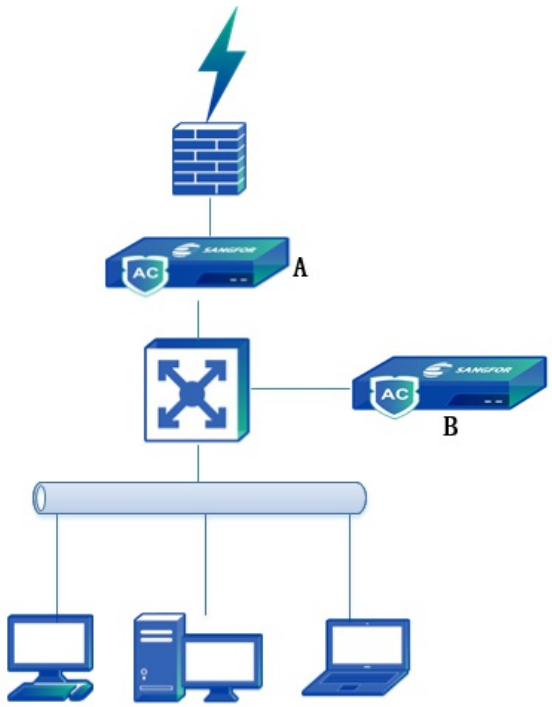
示例如下：

3. %192.200.244.96%基础情况。
4. %192.200.244.97:1775%加端口。
5. %2003::22%IPv6（上述1的IPv6场景）。
6. %[2003::22]:1773%IPv6加端口（上述2的IPv6场景）。
7. sxf%192.200.244.16%对控制器限制（指定某些控制器认证信息转发给指定设备）。
8. 10.10.10.20%192.200.244.96%对源IP限制（指定源IP认证信息转发给指定设备）。
9. 20.20.20.10;sangfor%172.16.12.1;172.16.12.4%多条件用分号隔开。

使用场景

AC设备能够和第二台AC/SG设备结合做认证，用户网络环境中部署了两台深信服设备，其中一台设备作认

证，另外一台设备作审计控制，只要用户通过了认证设备的认证后，审计控制设备就能够同步认证设备的用户信息，对用户进行审计控制，如图所示（设备A作认证，设备B作审计控制）。



数据流的过程如下：

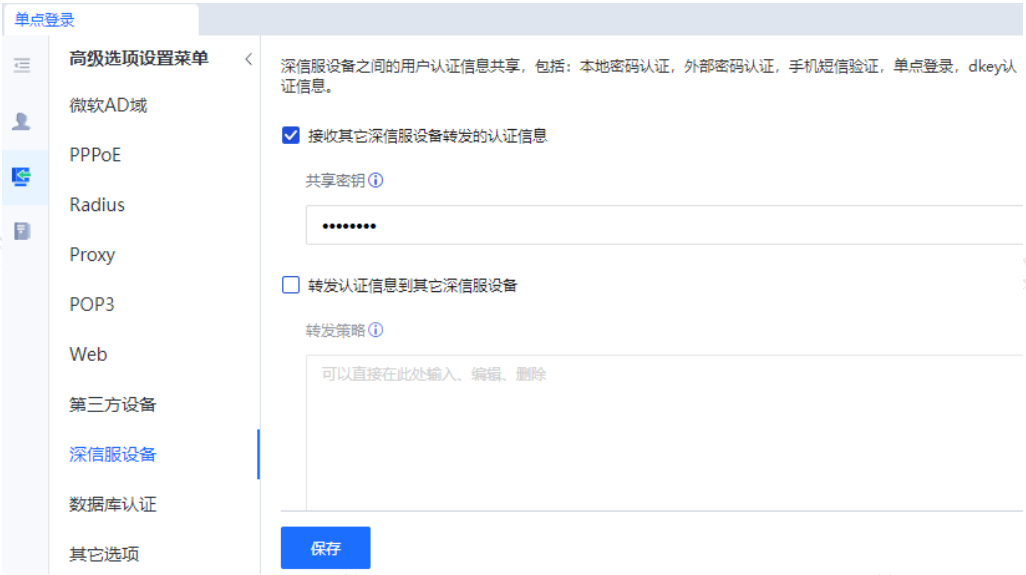
1. PC通过设备A的认证/注销。

2. 设备A通知设备B认证/注销用户，实现对用户进行审计控制。

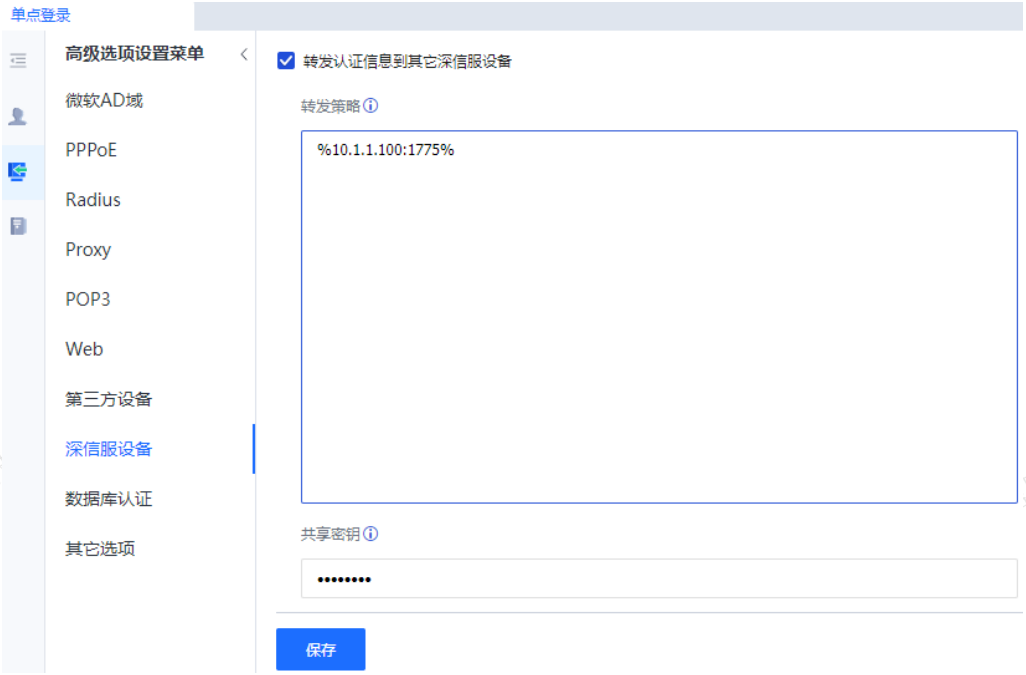
操作步骤

步骤1.根据需要使用单点登录的用户IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略]新增认证策略。

步骤2.在深信服设备B[接入管理/接入认证/PORTAL认证/单点登录/深信服设备] 勾选接收其他深信服设备的认证信息并设置共享密钥。



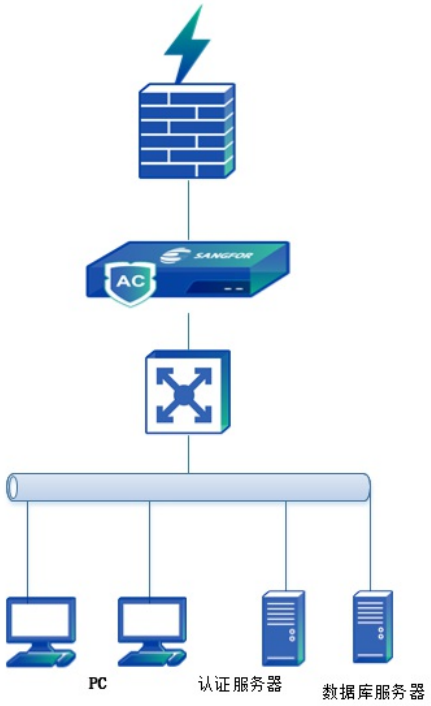
步骤3.对于网桥部署的深信服设备A，只需要启用[转发认证信息到其他深信服设备]并设置相应的设备IP和共享密钥。



这样深信服设备A就可以将认证信息发送给设备B，旁路部署的设备B可以接收深信服设备A转发过来的认证信息，保持和深信服设备A的认证信息相同。如果B是旁路部署的深信服上网优化设备，用户访问某些数据必须通过代理才能访问，代理服务器是使用深信服上网优化设备B有做代理设置和用户认证，这样用户只需要通过设备A的认证，就可以自动通过设备B的认证，使用代理方式来访问某些应用了，因为此时A和B的在线用户信息是相同的。

6.2.1.3.8.数据库认证

当网络环境中已有一套数据库系统存储并管理用户认证信息、组织结构的情况下，深信服AC设备支持配置SQL查询语句，查询该数据库系统中的用户列表和已认证用户，并同步到设备的组织结构和在线用户列表中，从而支持和数据库系统结合的单点登录，实现用户通过数据库认证后，即通过AC设备的用户认证，同时用户从数据库认证系统中注销，也自动完成在设备上的注销。目前支持的数据库类型有Oracle，mssql server，db2和mysql几种。



数据流的过程如下：

1. PC通过认证服务器的认证，在数据库服务器中更新PC的认证信息。

2. 设备定时查询数据库服务器中在线用户，并更新设备自身的在线用户列表。

3. PC使用AC设备获取到的在线用户身份上网。

操作步骤

步骤1.根据需要使用单点登录的用户IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略]新增认证策略。

步骤2.设置数据库服务器，点击进入[接入管理/接入认证/PORTAL认证/认证服务器]进行设置（参见数据库认证章节）。

在[接入管理/接入认证/PORTAL认证/单点登录/数据库认证]页面勾选[启用数据库认证单点登录]，选择数据库服务器并设置SQL查询语句。

数据库服务器：选择步骤1设置好的数据库服务器。

获取已认证用户列表的sql语句：设置可以查询到在线用户的select语句，设备通过该select语句查询数据库中的用户信息表来获取在线用户。

说明：

sql语句返回的结果集不能超过2列，第一列为用户名，第二列为IP地址，能查询的记录数不能超过200000条。

获取已认证用户列表的时间间隔：默认值是30s，指用户通过认证服务器认证到通过AC认证之间的最大时间间隔。

点击<测试有效性>列出可以获取的信息。

说明：

1．在线用户列表只支持同步“用户名”和“IP”，不支持同步其他用户属性，如用户是否禁用、是否过期等，默认同步过来的用户是启用和永不过期的。

2．数据库认证支持用户自动同步，具体请参见[用户管理/用户自动同步]。

3．在某些情况下，用户通过认证服务器认证之后在一个时间间隔后（取决于[获取已认证用户列表的时间间隔]设置）才会通过AC的认证，建议认证策略设置单点登录失败时选择[不需要认证]的认证方式。

6.2.1.3.9.其他选项

其他选项用于登录服务器的数据不经过网关，则需要设定监听镜像网口，监听登录的数据，勾选一个空闲接口进行监听。这个监听口在域单点登录监听模式、Radius单点登录、POP3单点登录以及Web单点登录等方式时均可以设置。

此处的监听口还可以用于设备旁路部署模式下，监听镜像上网数据。

认证页面定制

认证页面定制包括：认证页面和免责声明页面。

认证页面定制是在认证上网前，网页重定向到认证页面，该页面可自定义编辑定制，免责声明页面也能自定义定制。

认证页面

内置认证页面模板有：认证页面（无广告无免责声明）、认证页面（无广告含免责声明）、认证页面（含广告含免责声明）、认证页面（全屏广告）、定制认证页面（无广告含免责声明），内置模板不可以删除。

免责声明页面

内置认证声明页面模板有：免责声明页面（无广告）、免责声明页面（含广告）、免责声明页面（全屏广告），内置模块不可以删除。

管理员可上传定制页面，点击<上传页面>，用于上传认证页面模板。

权限设定：开启这个选项后，除了admin管理员，其他管理员都只能编辑自己有权限的页面。

授权给：在开启了独立权限控制后，用于给非admin管理员，授权可以编辑的页面。

编辑认证页面操作举例：

步骤1.点击任意一个页面模板名称，出现如下编辑页面。（如认证页面含广告免责声明）为例。

步骤2.管理员编辑选项中的页面标题、LOGO、背景颜色、页面文字、广告图片轮播、免责声明在页面上的对应位置。

步骤3.点击<背景颜色>在左上角选择颜色，编辑完毕后点击<确定>，保存配置。

步骤4.点击<页面文字>，可编辑如下内容。

步骤5.广告图片轮播：可以上传多张图片，在认证页面轮播，并可以分别指定各张图片链接的网址。

步骤6.图片链接的网址会自动加到全局排除列表中，以保证用户在未通过认证前能访问。

步骤7.在[免责声明]处，点击<编辑>：在此处编辑免责声明，并可以设置：默认是否选中“我已经同意并阅读免责声明条款”。

步骤8.编辑完成后，点击<提交>，完成页面编辑。

说明

：

内置的页面模板因为页面中包含的内容不同，编辑项有所区别，以上配置以含广告含免责声明的页面编辑为

例，其他页面模板配置以实际页面为准。

802.1x认证

802.1x认证主要用于内网强管控场景，该场景的需求是在没有认证之前不能访问内网（包括二层网络也不能接入），也不能经过二层交换机。优点是做到严格的入网控制，如果没有认证，二层网络也无法正常接入，杜绝非法用户和非法终端接入网络，未通过认证则无法接入内网。

802.1x认证主要包括了802.1x入网控制、联动交换机、VLAN关联用户三大模块，主要用于设置802.1x认证的相关功能。

802.1X入网控制

802.1x认证主要用于内网强管控场景，该场景的需求是：在没有认证之前不能访问内网（包括二层网络也不能接入），也不能经过二层交换机。优点是做到严格的入网控制，如果入网未通过认证，则二层网络也无法正常接入。达到杜绝非法用户和非法终端接入网络的效果。

开启802.1X逃生功能：启用该功能需要同时在交换机上开启逃生VLAN功能。

若启用该功能，AC会把逃生以后的用户划分到逃生VLAN；

若该功能未启用且交换机上配置了且逃生VLAN，当AC宕机、长时间断开连接、终端用户会自动进入逃生VLAN，确保正常的网络接入。

说明：

请确认已在交换机上配置好逃生功能，交换机未配置逃生功能时开启802.1x逃生功能将导致终端无法接入网络。

基础设置

该配置设置AC作为Radius服务器使用的认证和计费端口，认证端口默认为1812，服务器密钥需与交换机上配置的密钥一致，计费端口默认1813。

准入客户端下载

更新准入客户端功能配置后请先点击提交再进行下载，客户端的安装包方式有两种：MSI安装包、EXE安装包。**（MSI安装包中内置AD域透明安装准入配置方法文档）**。

说明：

1.MSI安装的准入客户端无法防止卸载，通常用于结合域控推送。

2.EXE包用于准入客户端防卸载，需要结合[接入关联/准入客户端配置]中的<设置准入客户端卸载密码>使用。

认证方式

• 账号密码认证

可选本地用户和AD域账号。本地用户的用户来源为本地，需要在用户管理中新建本地用户。用户来源为AD域，AC设备本身需要加入域，客户端提交用户名密码后，由AC到AD域校验，AD域返回校验结果后再由AC根据结果通知交换机是否允许接入。

• 外部证书认证

用于企业已有CA证书中心且向用户签发了受信任的个人证书的情景下，AC结合企业的CA证书，在接入交换机上开启802.1X认证，入网终端在准入客户端上选择证书认证，然后导入企业签发的个人证书完成认证。

• AD域单点登录

适用于与企业现有的AD域进行无缝对接，当用户成功登录AD域后，自动通过AC与交换机的802.1X认证，不需要再次输入账号密码认证。

开启802.1X认证前重定向提醒

DNS重定向：配置DNS重定向功能来实现802.1X的认证前重定向功能，用于认证前推送准入客户端和自注册等功能。

服务器IP地址：用于DNS重定向的服务器IP地址必须与AC的DMZ管理口地址同网段，且不能复用管理口的IP地址。

TTL（秒）：默认为30秒，范围：1-86400秒。

提醒页面设置：用于设置提醒用户安装准入客户端页面。

认证后处理

认证后处理用来设置用户通过认证之后的用户组。

1. 选择非本地/域用户使用该组上线认证，在本地组结构中的用户，以本地组上线，非本地/非域用户才会以指定的组上线。
2. 自动录入用户到本地组织结构，其中属性值可选：允许多人同时使用、仅允许一个人使用。
3. 自动录入用户名MAC绑定并限制登录，详细配置参考用户绑定管理章节。当用户换了新终端需要审批请勾选用户使用新终端登录需审批。
4. 用户限制登录可选：仅允许以下用户登录，不允许以下用户登录、新增自定义用户匹配列表。

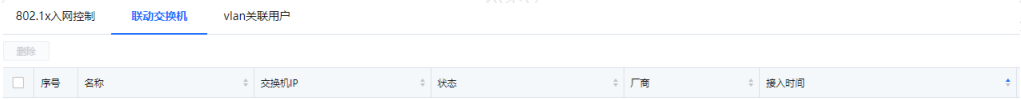
• 高级选项

启用强制注销用户功能：用于在AC上强制注销802.1X用户，启用该功能需要在交换机上配置RADIUS CoA/DM功能。（CoA报文用于在用户不下线的情况动态改变入网用户属性，DM报文用于中断用户连接。）

联动交换机

联动交换机在[接入认证/802.1x接入认证/联动交换机]，主要查看目前对接的交换机状态，其中包括交换机名称、IP地址、状态(是否在线)、厂商名称、接入时间等信息。

该页面无配置按钮，AC收到交换机发送的认证报文之后自动显示交换机相关信息。



VLAN关联用户

在[接入认证/802.1x接入认证/VLAN关联用户]，VLAN关联用户主要用于动态设置用户所属的VLAN，包括删除策略，启用/禁用和对策略上移下移设置。

点击<新增>可新增VLAN策略设置，填写策略名称、策略描述，适用用户是设置拥有动态VLAN权限的用户范围，VLAN ID是设置802.1x用户成功认证后的VLAN归属。

配置案例

某企业近期出现内网有未通过Portal认证的不明IP访问内网服务器读取机密文件的记录，需要对内网接入终端进行强管控，接入终端未通过认证前，内外网资源均不能访问，认证使用账号密码认证。确保终端入网均需认证，提高内网的安全性。

需求分析

该需求结合AC本地用户对接入终端做802.1x认证，交换机开启802.1x，终端输入AC本地创建的用户名和密码完成认证上线，未认证前接入终端不能访问内网资源。

• 802.1x认证需要先启用AC的802.1x入网控制功能，将AC作为Radius服务器，配置相应的端口和服务器密钥；

• 选择用户来源，可选本地用户和AD域用户；

• 最后配置认证后处理的策略，包括用户所属组，是否绑定用户，是否限制用户登录等配置。

操作步骤

步骤1.AC开启802.1x认证。

在导航菜单中的[接入管理/802.1x接入认证]点击开始配置。启用802.1X入网控制功能，并配置Radius认证端口为1812和计费端口为1813，服务器密钥为123。认证服务器启用本地密码认证。

说明：

1. 配置的 Radius端口不能与联动对接设置中Radius认证服务器冲突。

2. AC内置两套Radius服务器，802.1x认证使用Free Radius，联动对接设置中的Radius是在Portal对接中使用，两者端口不冲突的情况下可以同时开启。

3. 若冲突，请修改联动对接设置中Radius认证服务器的端口，配置为其他端口。

步骤2.当有认证数据发到AC时[接入管理/802.1x接入认证/联动交换机]会显示交换机的状态。

步骤3.在[接入管理/用户管理/本地组/用户]中点击<新增>按钮创建本地用户，填写登录名和密码并点击<提交>。

步骤4.对接交换机802.1x配置。

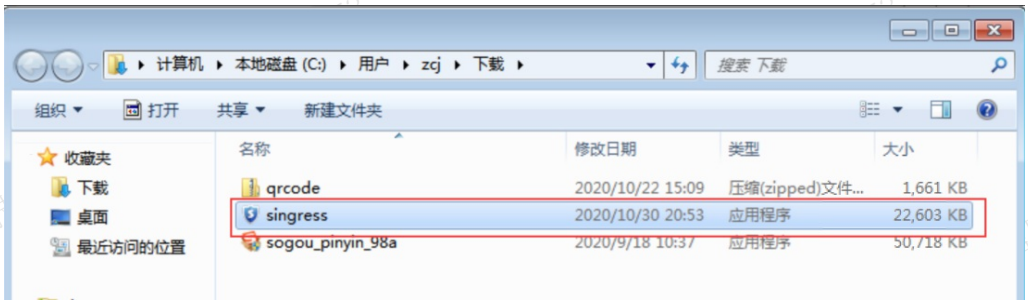
对应交换机启用802.1x功能，认证服务器选择radius，radius服务器指向AC，交换机配置请参考《交换机802.1x配置工具V2.0》。链接地址：https://bbs.sangfor.com.cn路径：自助服务/常用工具/交换机802.1x配置工具。该工具集成了多种主流交换机厂商配置。

步骤5.AC需要获取到终端的IP与MAC地址的对应关系用以用户上线。共有四种方式上线：1、交换机Radius计费报文携带IP信息并发送到AC（大部分厂商计费报文都会携带IP信息，如发现未携带，请联系厂商工程师）；2、交换机配置镜像口接入到AC镜像口流量上线；3、通过从ARP、DHCP报文获取MAC，或通过SNMP跨三层获取MAC地址；4、使用认证助手登录802.1x的终端会上报IP和MAC地址信息到AC设备。建议通过计费报文的方式。（若该厂商交换机计费报文中不携带IP，请参考SNMP配置章节）。

步骤6.认证助手配置。

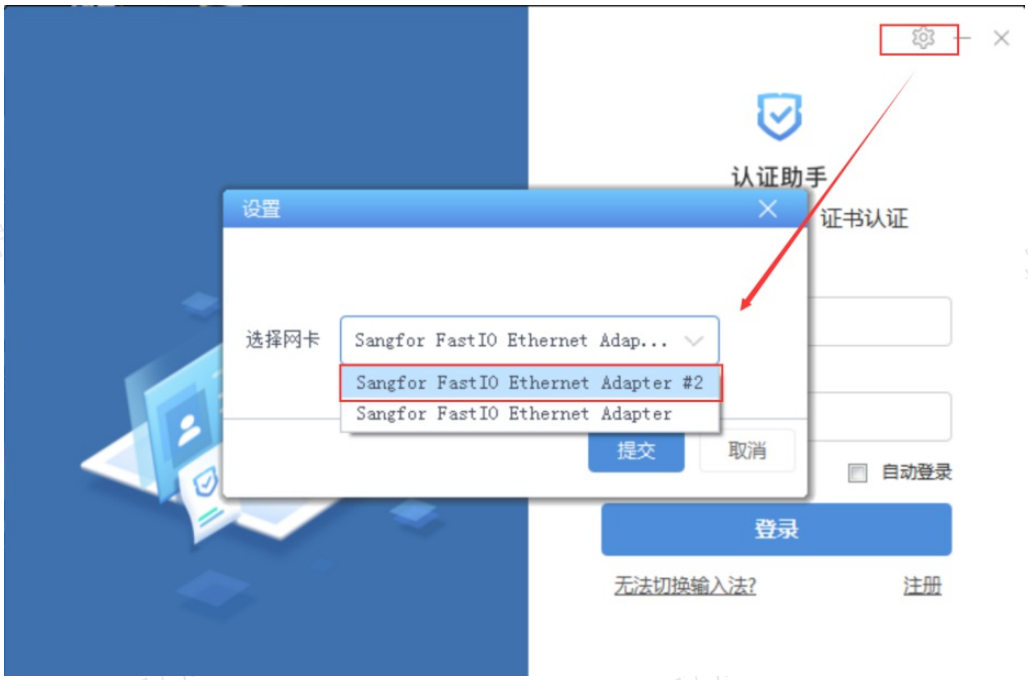
在[接入管理/准入客户端配置]中依次勾选[开启准入客户端802.1x功能]、[设置准入客户端卸载密码]并填写密码、[设置准入客户端网关地址]并在[网关主IP地址]中填入AC设备的IP地址、[系统推送准入客户端]、[允许上网]。（在AC控制台勾选[开启准入认证客户端802.1x功能]后下载的认证助手才会生成认证助手快捷方式，用于输入账号密码）。

步骤7.在AC设备Web控制台下载认证助手（准入客户端），以管理员权限安装singress.exe，注意勾选开启准入认证客户端802.1x功能才会生成快捷方式。



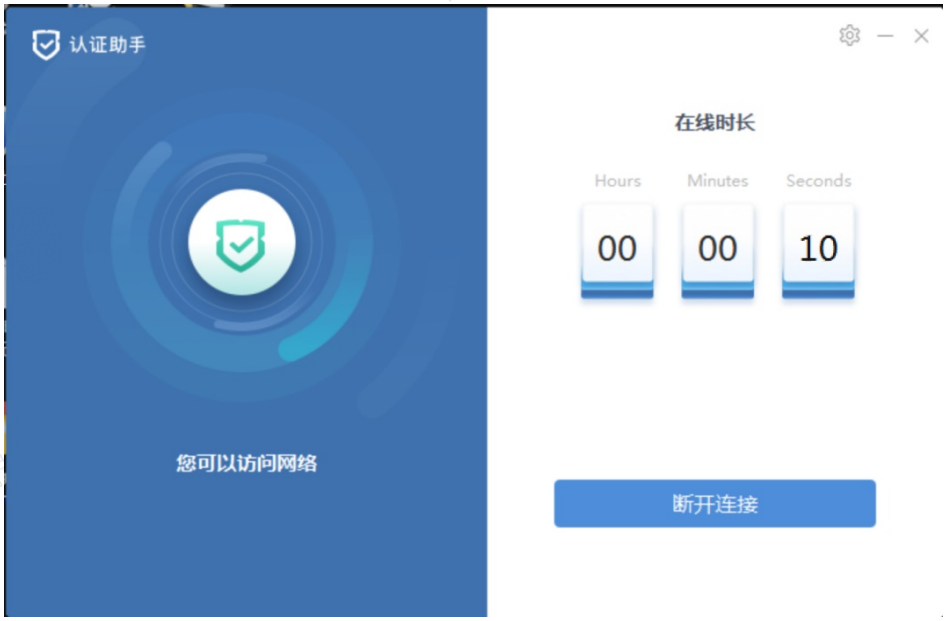
步骤8.安装完成之后会在桌面生成快捷方式，双击运行。 

步骤9.使用认证助手时注意右上角选择正确的网卡，并点击<登录>上线。



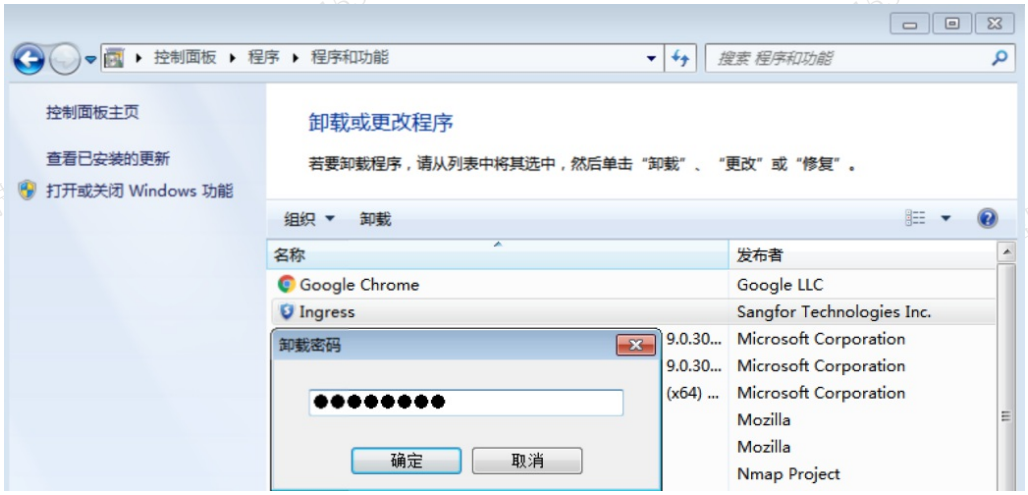
效果展示

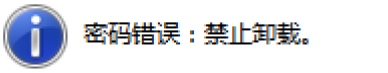
1. 用户在认证助手输入账号密码登录成功后会显示在线时长。



2. 在[全网监控/入网用户管理]的在线列表能看到用户的上线情况，认证方式为802.1x。

3. 在PC[控制面板/程序/程序和功能]中找到ingress程序会点击卸载会提示输入卸载密码。需输入正确的卸载密码（准入客户端配置中设置的准入客户端卸载密码）才能卸载程序，否则提示“密码错误：禁止卸载”。





说明：802.1X详细配置（包括802.1x+AD域用户、802.1x+CA认证、MAB免认证等场景配置）请参考文档《深信服全网行为管理准入功能配置指导》

链接地址：https://bbs.sangfor.com.cn

路径：知识库/资料库。

联动对接设置

联动对接设置主要用于对接第三方设备，包括控制器对接、Radius认证服务器、跨三层取MAC三大模块。

控制器对接

控制器对接包括深信服设备对接和第三方控制器对接，适用于多分支场景。其中深信服设备对接用于总部AC作为认证中心的时候，结合分支深信服设备做认证托管统一推送认证页面。第三方控制器用于AC做统一认证服务器时，对接无线控制器实现统一认证页面推送，实现统一认证，权随人行。

深信服设备

用于AC作为认证中心的时候，对接深信服设备完成认证托管功能。

认证中心设置：用于设置认证中心参数。

- 接入密钥：用于分支AC接入的密钥，需与分支深信服设备的对接密钥保持一致。
- 通信端口：用于AC认证中心与分支深信服设备通信的端口，默认为390，可修改，需与分支深信服设备的认证中心端口保持一致。

说明

：

AC认证中心完成配置后，需到分支AC/SG设备配置认证托管，可参考认证托管章节。有BBC环境配置请参考多分支组网场景章节。

第三方控制器

<新增>按钮添加一条新的对接第三方控制器策略。

控制器信息

- 名称：用于设置第三方Portal服务器的名称。
- 描述：对服务器的描述信息。
- Portal协议：支持的Portal协议类型，目前支持和标准的CMCC1.0、CMCC2.0、华为Portal 2.0/IMC协议、cisco外部Portal web认证协议、Aruba协议对接。
- 对接URL：选择相关的协议之后，会自动生成一个URL地址。
- 控制器IP：第三方Portal控制器的IP地址，可填写端口，如果不填写端口号和认证中心对接的时候默认使用2000端口。
- 使用外部Radius服务器认证：认证中心结合第三方控制器认证，当用户信息维护在第三的方Radius服务器上面的时候，需要勾选；当认证中心本身充当Radius服务器的时候，则不需要勾选，但是需要在[接入管理/接入认证/联动对接设置/radius认证服务器]启用认证端口和设置共享密钥。

客户端参数字段配置

- IP地址字段：从数据包获取或者是从URL参数获取。
- MAC地址字段：第三方控制器的mac地址信息。
- vlan1字段和vlan2字段：第三方控制器数据包含的字段信息。
- bssid字段：和控制器保持一致。
- 认证前URL字段：和控制器保持一致。

当有多条第三方控制器的信息配置的，可以利用右上角的搜索框来搜索。

Radius认证服务器

当需要把设备作为Radius认证服务器时，需要勾选<启用>，然后设置认证端口、计费端口及其共享密钥，点击<提交>，即可将AC配置为Radius认证服务器，默认只支持PAP（密码认证协议）。

说明：

计费端口与认证端口使用相互独立的密钥。

认证端口：默认为1812，可修改。共享密钥设置和对接的设备一致。

计费端口：默认为1813，可修改。共享密钥设置和对接的设备一致。

跨三层取MAC

跨三层取MAC主要功能是AC设备作为SNMP的客户端通过SNMP协议向客户内网三层设备（作为SNMP服务器）获取IP和MAC的对应关系，来实现过三层网络设备后，设备依然正常识别终端用户的MAC地址。跨三层取MAC提供两种方式。

第一种：通过镜像读取内网用户的MAC（推荐）。

勾选<抓取ARP包或者DHCP包获取MAC>，将AC任意一个空闲的网口接到交换机，交换机对应的接口启用镜像，将相关数据包镜像到AC，此方法不需要交换机启用SNMP协议。

第二种：配置跨三层取MAC。

内网用户绑定MAC地址或者限定了用户的MAC地址范围，并且内网是跨三层的环境下，需要启用<跨三层取MAC>的功能，用于获取内网用户的MAC地址。使用此功能的前提是内网交换机支持SNMP功能，AC通过SNMP协议获取交换机上内网用户真实的MAC地址。

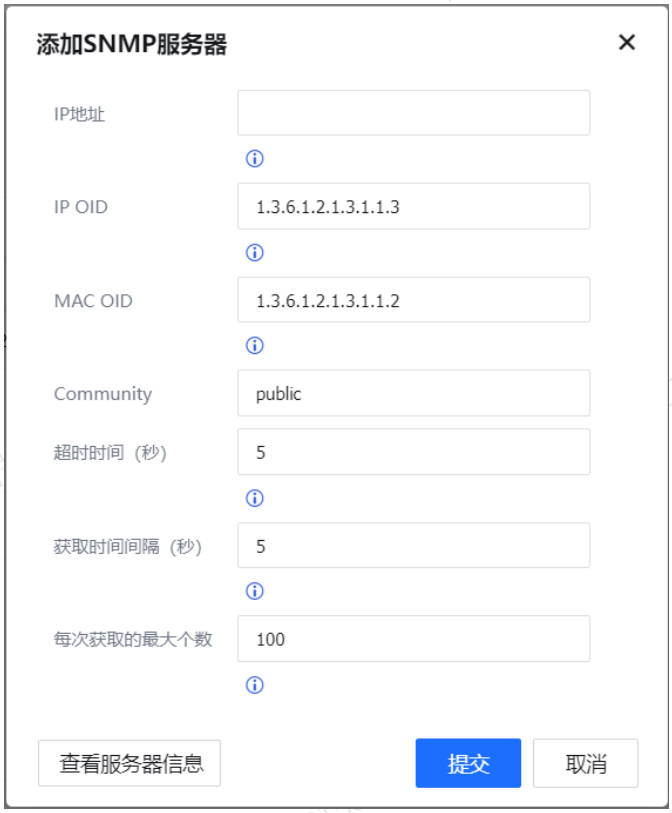
原理：设备上会定期发SNMP Request到三层交换机请求交换机的ARP表，并保存在设备内存中。此时如果三层交换机其它网段的电脑经过设备上网时，如一台PC 192.168.1.2（和设备LAN口不在同一网段）经过设备上网，该PC数据包经过设备时，设备校验此数据包的MAC是三层交换机的MAC，则对此MAC不做处理，而根据192.168.1.2这个IP去内存中查找其真实的MAC地址，实现对用户真实MAC的验证。

操作步骤

步骤1.在三层交换机上开启SNMP功能，且需要配置读取权限的团体名。

步骤2.在[接入管理/接入认证/Portal认证/联动对接设置/跨三层取MAC]进行设置，在设备界面勾选<启用跨三层MAC识别>。

步骤3.在[SNMP服务器列表]点击<新增>把需要获取MAC地址的三层交换机信息，配置完成，点击<提交>即可。



• IP地址：**填写交换机IP地址，一般是PC网关设备。**

• IP OID和MAC OID：**默认OID是标准的，不需要修改，标准的SNMP协议均支持，可根据不同厂商设备的OID修改。**

• Community：**只读权限的团体名称即可，与交换机配置一样即可。**

• 超时时间：**设置AC获取SNMP信息的超时时间。**

• 获取时间间隔：**设置AC多久发一次SNMP请求获取信息。**

• 每次获取的最大个数：**设置每次获取的SNMP条目的最大个数。**

步骤4.点击<查看服务器信息>，用于查看SNMP服务器即交换机的上的SNMP信息，可测试能否从交换机获取PC的IP和MAC，有返回结果则能正常获取。

步骤5.填写内网交换机的MAC地址，避免这部分MAC被用户绑定。

步骤6.除了上一步手动填写交换机的MAC地址外，设备还可以自动发现三层交换机的MAC地址。

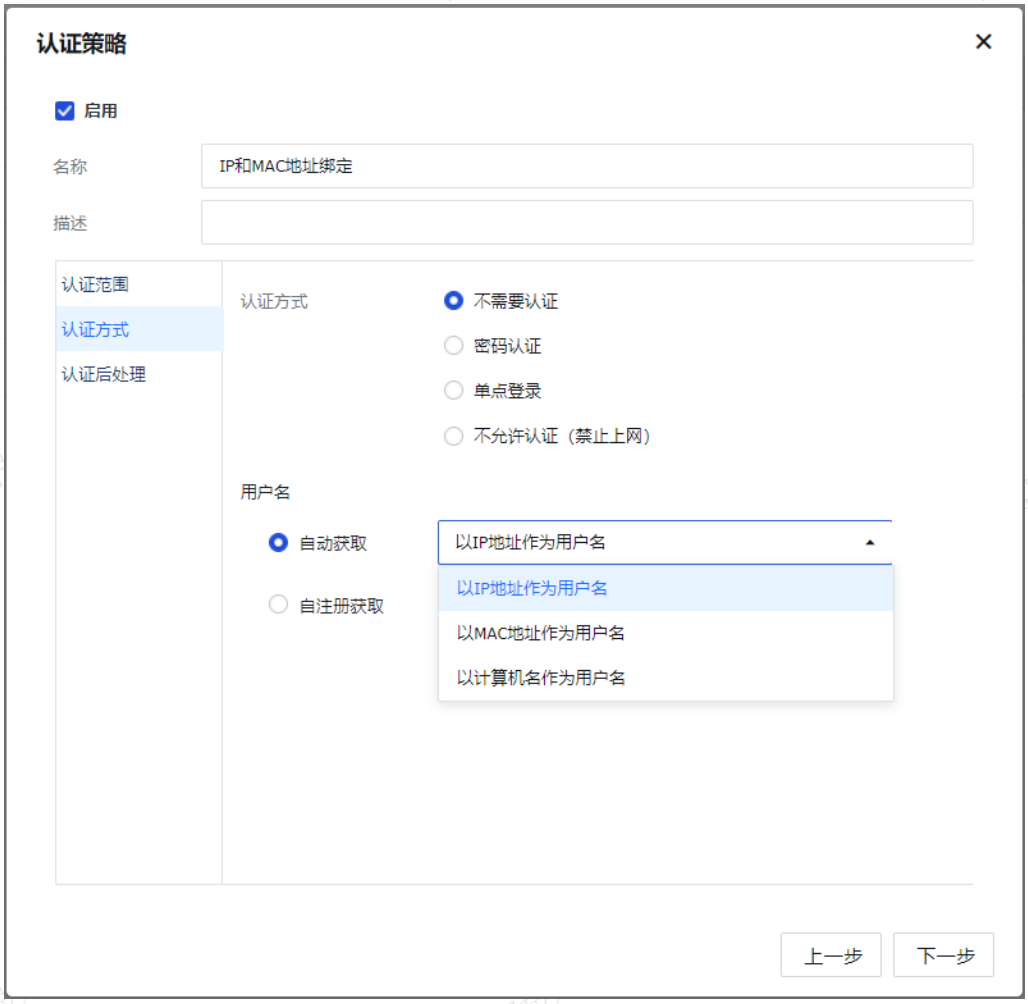
步骤7.点击<查看每MAC统计结果>查看统计的结果。当客户不清楚自己三层交换机地址，如果是三层MAC，当一个MAC对应多个不同的IP地址，AC会统计出十分钟内每个MAC对应的IP，可根据查看MAC统计结果，找到对应一个MAC的记录将MAC添加到排除列表。

步骤8.如果勾选[自动添加排除MAC]，设备会根据设置的[IP地址记录数]，自动将超过IP记录数的MAC地址添加到MAC地址排除列表中。

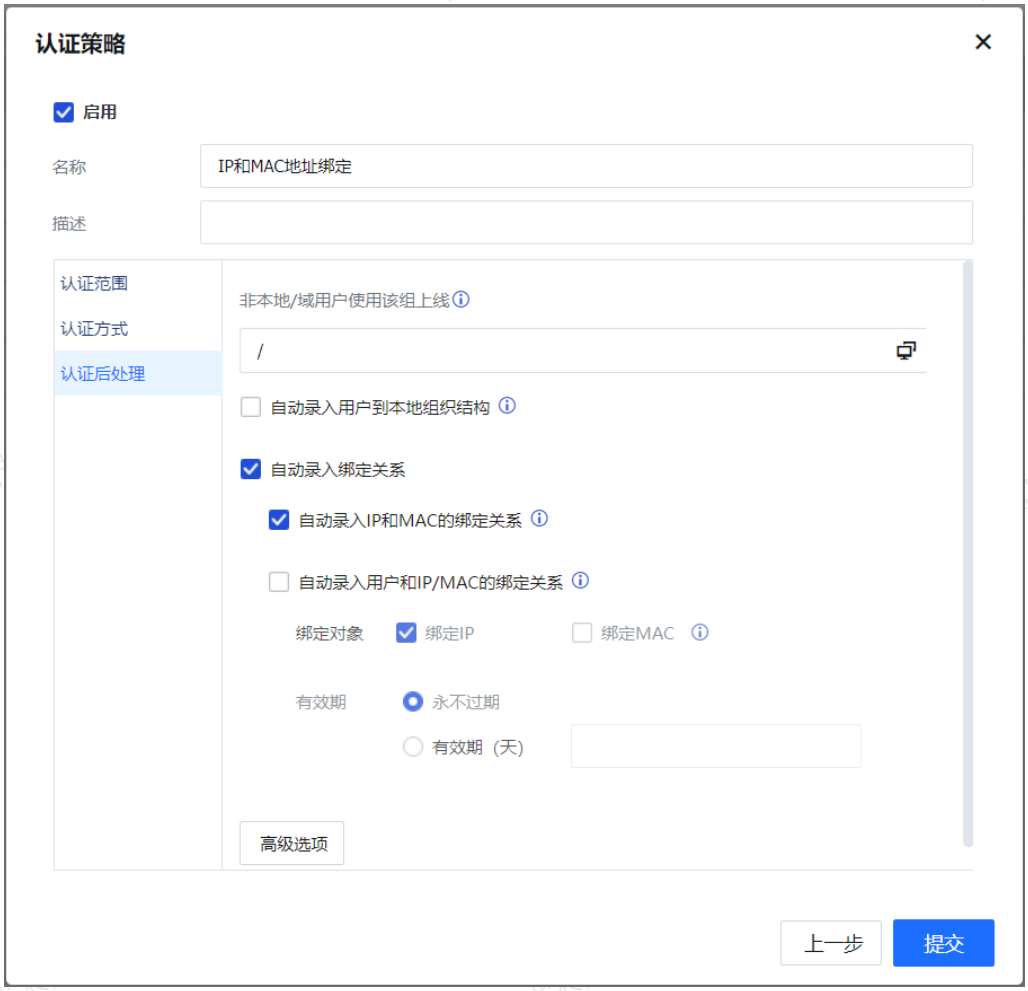
步骤9.勾选[自动添加排除MAC功能告警]，用于在自动添加MAC后，发送告警邮件给管理员。告警选项在[系统管理/系统配置/告警选项]中设置。

步骤10.在[接入管理/接入认证/PORTAL认证/认证策略]，点击新增一条策略，启用该策略，配置认证范围：填写测试PC所在的网段。支持根据IP地址段、MAC段匹配认证策略。

步骤11.认证方式选择不需要认证，用户名推荐选择以IP地址作为用户名。



步骤12.认证后处理选择自动录入绑定关系，其他设置根据自定义需求设置。



步骤13.点击<提交>，AC和三层交换机的配置已完成。

认证高级选项

认证高级选项包括认证选项、认证托管。

认证选项

认证选项用于配置跟认证相关的选项设置。

用户管理

• 自动注销无流量的用户：**设置一个超时时间（10-65535分钟），用户超过此超时时间没有流量则自动注销该用户。**

• 每天强制注销所有在线用户：**设置一个固定时间，每天定时将所有在线用户注销，该注销功能全局生效，启用时请慎重考虑。**

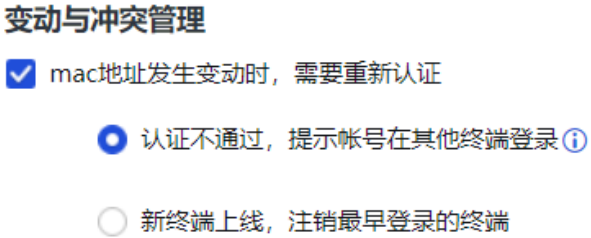
• 冻结持续认证失败的用户：**设置当超过认证失败次数（1-255次）时，冻结该用户的时间（1-1440分钟）**。

• 自动删除长久未登录的用户：**开启此功能后，会自动删除连续N天（1-365天）未登录的用户及其设备，只会删除自动登录的用户，不会删除手动创建的用户。**

• 自动删除过期的免认证绑定关系：**对于设备自动录入的免认证绑定关系，检测登录时间，如果是免认证时间过期，则会自动删除这些用户。手动录入的免认证用户也会删除。**

• 单用户绑定终端个数限制：**用于设置用户对应的终端数,这里限制的是一个用户能在几个终端上登录。**

变更与冲突管理



• MAC地址发生变动时，需要重新认证：原本认证通过的用户，MAC地址变化了会要求重新认证。比如一个IP为192.168.1.1的用户，认证方式为用户名和密码认证，当这个用户下线后，由于在一段时间内不会注销该用户，这时另一个用户把IP改成192.168.1.1，这样MAC地址就发生了变化，需要重新认证方可上网。

• 不允许多人同时登录的账号，如果认证时发现已经在其他IP上登录，则：对于不允许多人同时登录的账号，如果该用户已经在AC设备上线，在其他终端上仍然使用该用户账号登录，那么可以选择“认证不通过，提示账号在其他终端登录”或“新终端上线，注销最早登录的终端”。

• 公共账号允许多人同时登录，在[权限策略/用户限额策略]中可以设置公共账号允许登录的终端数，当终端数超限时，针对新上线的终端可以在此处选择上线策略，分别可以选择[认证不通过，提示账号在其他终端登录]、[新终端上线，注销最早登录的终端]。

说明：

802.1x认证暂不支持该功能。用户进行802.1x认证时，即使账户已经在其他IP上登陆，也能够上线。

免认证设置

启用Cookie免认证：设置Cookie免认证有效期，范围：1-100天。

使用场景：使用AC用户名密码认证时，实现在同一台PC上成功认证一次后，后续直接上网，不需要再重复输入用户名密码。

说明：

1. 首次登录时需要勾选记住登录状态

2. 在免认证有效期内请勿清除浏览器Cookie。

3. Cookie免认证的用户应该要设置为公有用户。如果是私有用户，新认证的用户会踢掉最早认证的用户下线，导致AC把该用户的Cookie数据清除。

安全设置

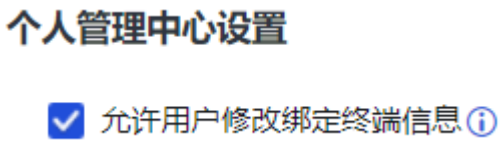
• 用户密码强度：**用来设置用户名密码认证时，密码的安全要求，可以选择：密码不能等于用户名、新密码不能与旧密码相同、限制密码最小长度、密码必须包括，这几项如果同时勾选则需要同时满足这几个条件，用户才能成功修改登录密码。**

• 采用SSL加密方式提交用户名和密码：**密码认证页面默认是HTTP页面，通过这个页面提交用户名是明文的方式，如果客户要求页面采用SSL加密的方式，需要勾选此项。**

• 域名：**密码认证页面的URL默认是设备IP地址的形式，如果需要以域名的形式显示则需要在此处定义好域名，同时需要在用户内网的DNS上添加A记录，将该域名指向设备的IP地址。**

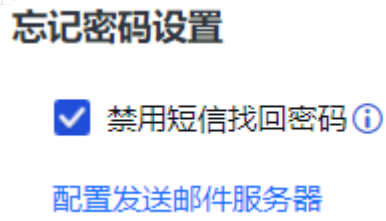
• 服务器证书：**导入或者创建SSL证书。在此处导入企业证书或者是创建相应的证书然后导入终端后可以将密码认证界面转变为https界面。**

个人管理中心设置



允许用户修改绑定终端信息：如果允许终端用户自己修改绑定终端信息可勾选此功能。

忘记密码设置



[禁用短信找回密码]：如果在用找回密码功能，不想使用短信找回密码，期望使用邮箱账号密码功能，可以勾选此功能。需要配置发送邮件服务器，详细请参考通知设置中的邮件发送服务器。

其他选项

• 未认证或被冻结时允许访问DNS服务：**用于允许在用户通过认证前或冻结后访问DNS服务。**

• HTTPS请求通过认证时，重定向到认证页面：**对于密码认证的用户，认证前上网打开HTTP网页会重定向到认证页面，但如果访问HTTPS网页则默认不会重定向，如果需要对HTTPS网页也重定向的话，需要勾选此项。需要将AC的根证书导入到终端，否则浏览器打开认证界面时会有证书错误告警。**

• 代理上网时，密码认证使用WEB认证页面：**若勾选，则代理上网时，密码认证使用WEB认证页面，若不勾选，则代理上网时，使用407(407 Authorization Required)弹框进行认证。**

• 域账号附加域名作为用户名：**当客户环境中存在多个域时，可以勾选此项，用于区分不同域服务器的用户，在在线用户列表、实时状态等页面可以看到用户后面加上了域名后缀。**

示例：某企业存在两个域：ACtest.com和ACCtest.com，两个域都作为域用户认证源，勾选该功能项后，入

网用户会以xxx@ACtest.com和xxx@ACCtest.com显示。

• WAN->LAN方向的连接不认证：代理服务器单臂部署，AC网桥部署在内网和代理服务器之间时，这种环境会有公网IP地址加到在线列表，需要勾选此项避免公网IP认证。

• 关闭组/用户排序功能：组/用户查询速度较慢，可以启用关闭组/用户排序功能来提高查询的速度。

• 将认证的虚拟域名（oauthservice.net/onauthservice.com）解析到指定IP地址）：环境中存在多台AC/SG场景配置Oauth认证或二维码认证，建议配置此功能。

认证托管

认证托管主要用于各分支AC、IAG设备将用户认证托管在总部认证中心AC实现统一认证。

• 认证中心IP地址：**填写认证中心的IP，支持IPv4和IPv6。**

• 对接密钥：**和认证中心设置的密钥保持一致。**

• 认证中心端口：**默认是TCP390端口，可在认证中心自定义，需与认证中心保持一致。**

• 重定向端口：**认证重定向页面使用到端口，默认是TCP80端口，可自定义。**

• LDAP服务端口：**统一认证中心做LDAP服务器开放的端口，默认是TCP389端口。**

• 逃生机制：**认证托管后支持逃生策略配置，在认证中心离线情况下，设备使用逃生机智的配置策略进行认证上线。逃生策略支持不需要认证和密码认证2种方式。**

• 不需要认证：**可以选择以IP、MAC、计算机名做用户名。可勾选<认证中心恢复正常时，不需要认证的用户需要重新认证>。**

• 密码认证：**选择认证服务器、认证页面和认证后跳转。配置参考认证策略配置。**

• 逃生时上线组：**当认证中心离线时，定义使用逃生机智的配置策略进行认证上线到用户组。**

• 点击测试有效性：**用于测试设备和统一认证中心的通讯情况。**

点击<提交>后，分支设备已经被托管到认证中心，并且可以跳转到认证中心。

认证中心显示设备接入状态。

说明：

1．开启认证托管后，认证相关功能在统一认证中心实现，在被认证托管设备上认证策略、用户绑定、IP/MAC绑定、用户自动同步、单点登录、认证控制器、Radius认证服务器功能将被隐藏并且功能不生效。

2．认证托管状态下，在分支AC上线的用户不支持同步上线到认证中心，但是在分支AC上注销的用户，可以同步在认证中心注销。

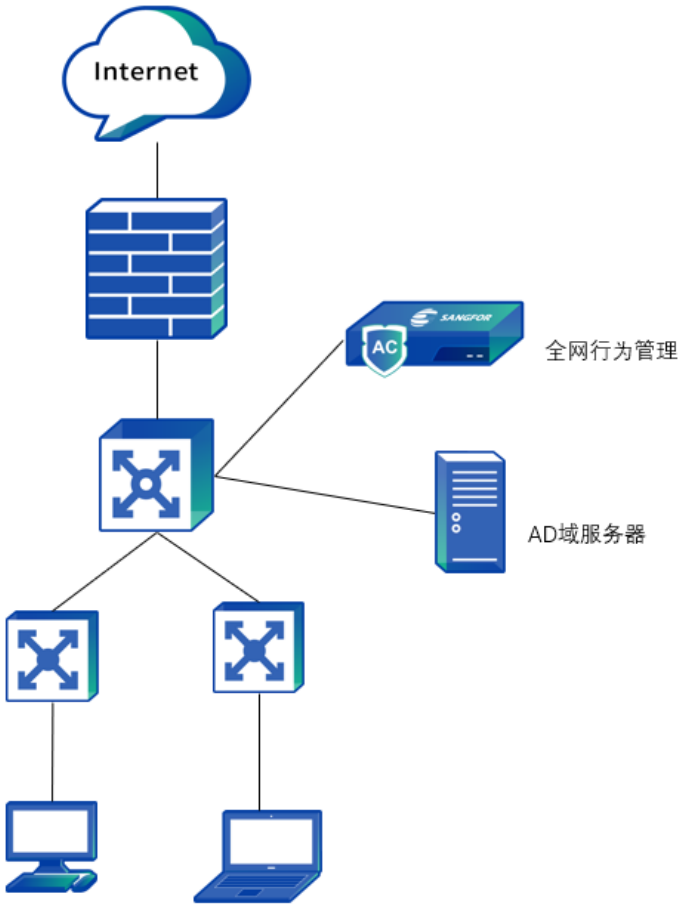
3．认证托管支持MAC免认证、不需要认证、密码认证、不允许认证4种认证策略方式。

4．认证托管功能支持控制设备自身作为代理服务器场景，支持HTTPS代理、HTTP代理、SOCK5代理场景。

接入认证AD域典型案例

802.1x场景结合AD域入网认证

该场景是结合AD域用户对接入终端做802.1X认证，交换机开启802.1X，终端输入AD域上的用户名和密码完成认证。



配置思路：

1. 确保AC与AD域能正常通信，AD域已经创建相应域用户。
2. AC和交换机完成802.1x配置并成功对接。
3. PC在AC设备下载认证助手并完成安装。

配置步骤

步骤1.AC开启802.1X认证：

勾选启用复选框，并配置Radius认证和计费端口；另外，这里配置的 Radius端口不能与联动对接设置中Radius认证服务器冲突（**AC内置两套Radius服务器，802.1X认证使用FreeRadius，联动对接设置中的Radius是在Portal对接中使用，两者端口不冲突的情况下可以同时开启**）；若冲突，请修改联动对接设置中Radius认证服务器的端口，配置为其他端口。

步骤2.点击导航菜单中的[接入管理/接入认证/802.1X接入认证]，勾选启用按钮开始配置。在[认证服务器]启用[AD域账号]认证。如下图所示：

步骤3.设置AC设备加入域的计算机名，后四位固定为网关序号的后四位，前面的字段可以用户自己定义，只支持字母，数字以及连接符“-”，最多支持10个字节。域名为需要加入域的域名，设置域对应的DNS服务器IP地址。设置AC加入AD域使用的域账号和密码，该账号要具备Domain Admin的权限，不一定需要administrator账号。

步骤4.点击测试有效性，检测各个参数是否有效，测试通过后点击提交。如果域服务器是Windows Server 2000以前的版本，还需要在[高级选项/配置]这里设置下域名。

步骤5.对接交换机802.1X配置：

对应交换机启用802.1x功能，认证服务器选择radius，radius服务器指向AC，交换机配置请参考《交换机802.1x配置工具V2.0》。链接地址：https://bbs.sangfor.com.cn路径：自助服务/常用工具/交换机802.1x配置工具。

步骤6.使用户能在AC上线：可以通过交换机配置计费报文带IP或者镜像口方式，接入到AC镜像口，通过抓取ARP或者DHCP包获取mac，也可以通过SNMP获取MAC地址。

步骤7.配置SNMP服务器，需要交换机开启相关服务。

步骤8.认证助手配置（这里介绍通过手动安装MSI包来安装准入客户端）

到AC平台下载准入客户端，如下图。

步骤9.解压之后以管理员权限安装singress.msi，注意勾选开启准入认证客户端802.1X功能才会生成快捷方式。

步骤10.安装完成之后会在桌面生成快捷方式。

效果展示

1. 使用域账号密码登录成功，会显示在线时长。

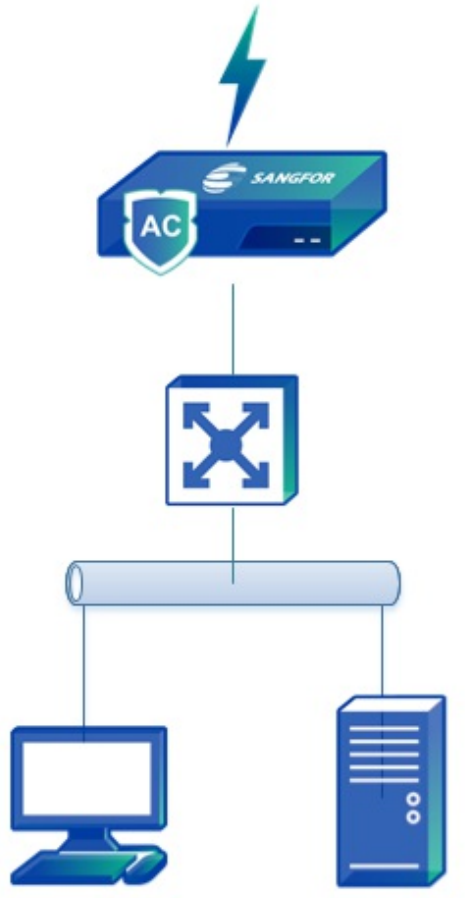
2. 在[入网管理/在线用户管理]可以看得在线用户的情况和认证的方式。

注意 ：

PC配置了802.1X认证，但是认证不成功，可以用抓包工具来抓包，看数据是否发到交换机，筛选条件为eap||eapol认证助手只支持Windows客户端。

通过域下发登录脚本的单点登录

通过配置域服务器登录（logon.exe）和注销（logoff.exe）脚本，在用户登录或注销域时通过下发的域策略执行登录或注销脚本，执行脚本的同时完成用户在设备上的登录和注销。如图所示。



数据流的过程大致如下：

1. PC请求登录域。
2. 域返回成功登录信息给PC。
3. PC运行logon.exe并上报 成功登录域的信息给设备。

配置案例：要求对内网172.16.1.0/24网段的用户使用AD域单点登录的认证方式，认证成功后以域账号上线；并且删除将用户和IP进行自动绑定；当单点登录失败时跳转到认证页面通过手动输入AD域账号和密码进行认证。

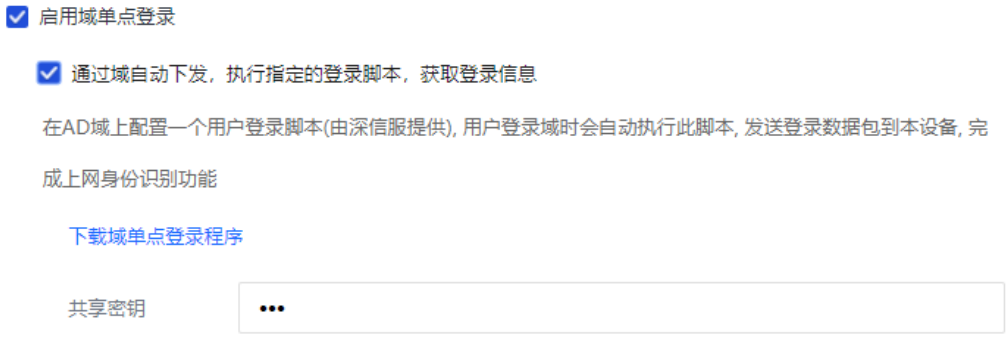
操作步骤

步骤1.设置认证AD域服务器，点击进入[接入管理/接入认证/PORTAL认证/认证服务器]进行设置（参考LDAP服务器章节）。

步骤2.根据需要使用单点登录的用户IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略]，点击新增认证策略，勾选启用，填写名称。

步骤3.设置认证范围，填写适用范围：172.16.1.0/24。设置认证方式，认证方式选择单点登录，单点登录失败的用户勾选密码认证，认证服务器选择LDAP。

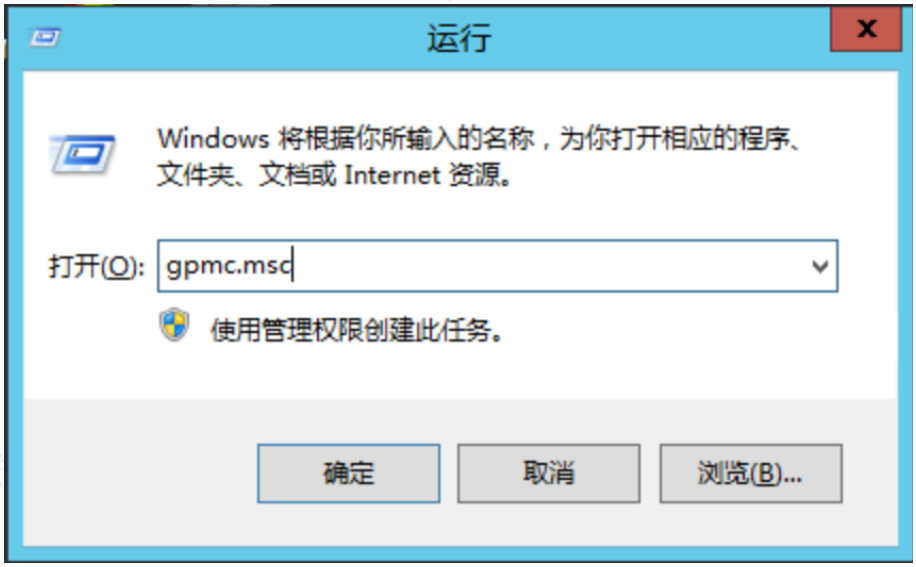
步骤4.在[接入管理/接入认证/PORTAL认证/单点登录选项/微软AD域] 勾选[启用域单点登录]和[通过域自动下发，执行指定的登录脚本，获取登录信息]，并设置共享密钥。



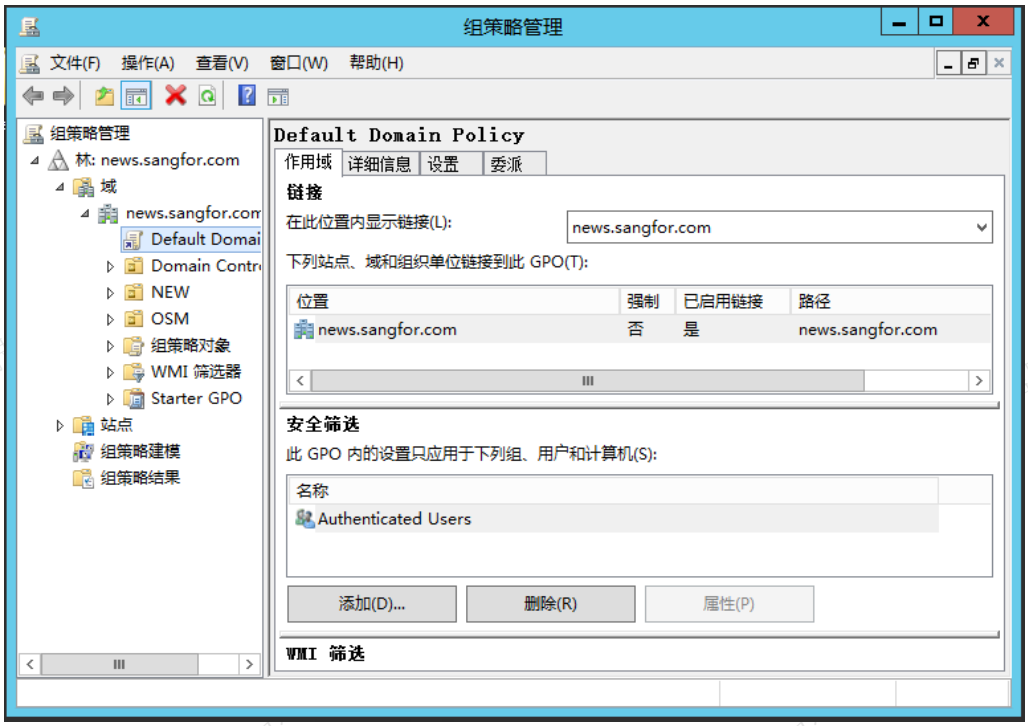
步骤5.在[共享密钥]中输入共享密钥，共享密钥用于AD域服务器和设备的加密通讯，需要在登录脚本中设置相同的共享密钥。点击<下载域单点登录程序>下载登录注销脚本，下载脚本。

步骤6.在AD域服务器上配置登录脚本程序。

1. 登录域服务器后，使用WIN+R在运行中输入gpmc.msc打开组策略管理，如下图。

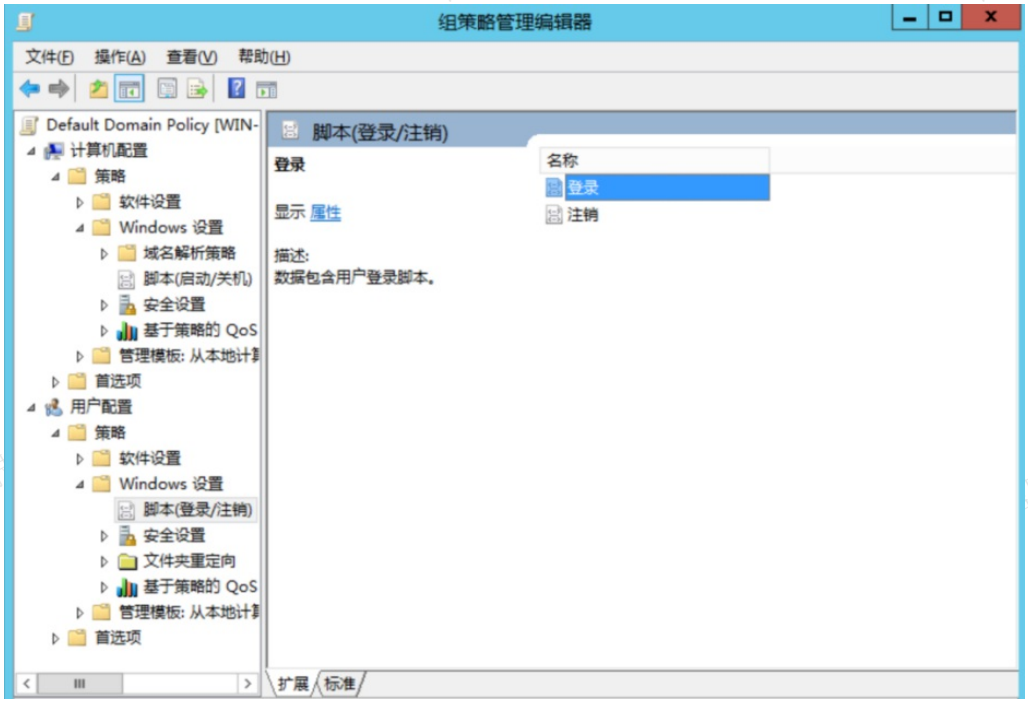


2. 策略管理页面如下所示。

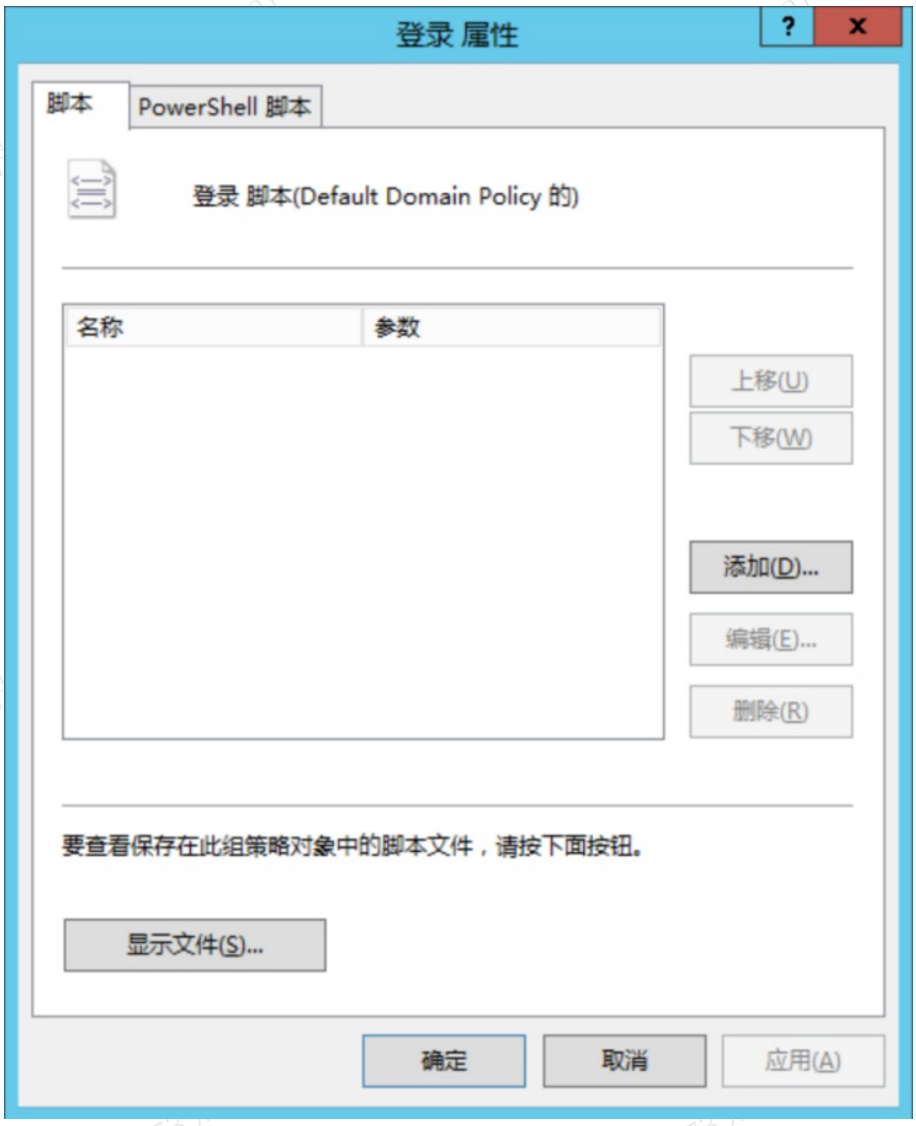


3. 在弹出的窗口中，右键选中组策略“Default Domain Policy”，点击<编辑>打开组策略管理编辑器。

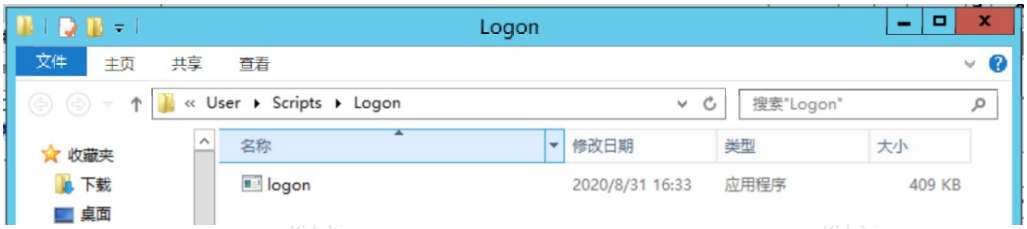
4. 在弹出的组策略编辑器中依次点击[用户配置/Windows设置/脚本(登录/注销)]。



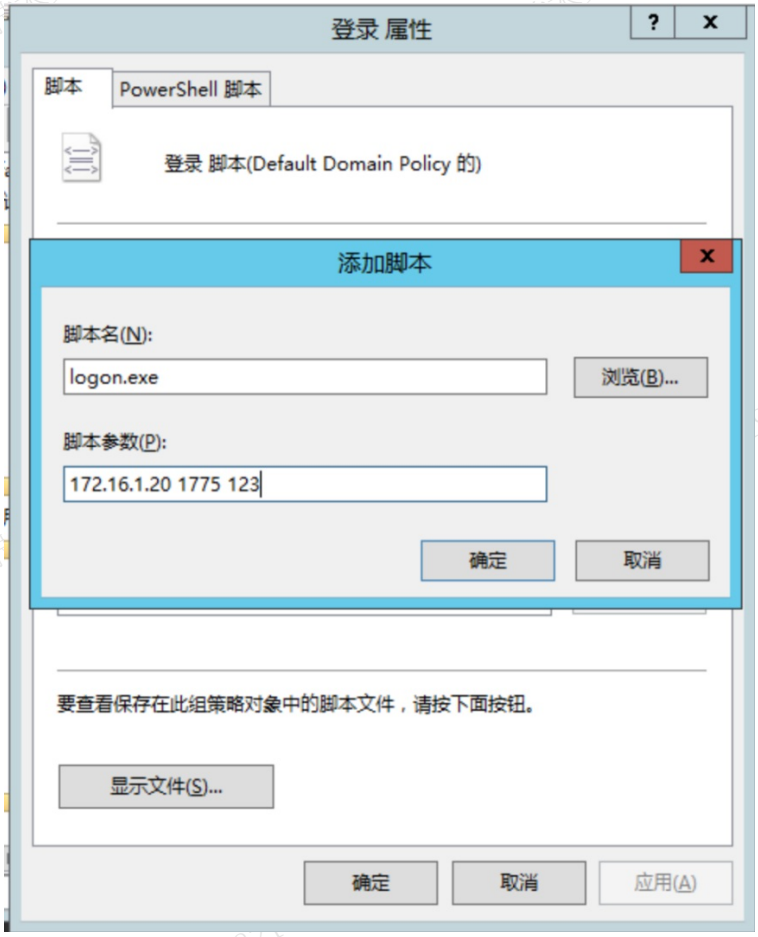
5. 双击右边的<登录>选项，在弹出的登录脚本编辑窗口左下脚，点击<显示文件>，会打开一个目录然后，将登录的脚本保存在该目录下。



6. 关闭该目录。

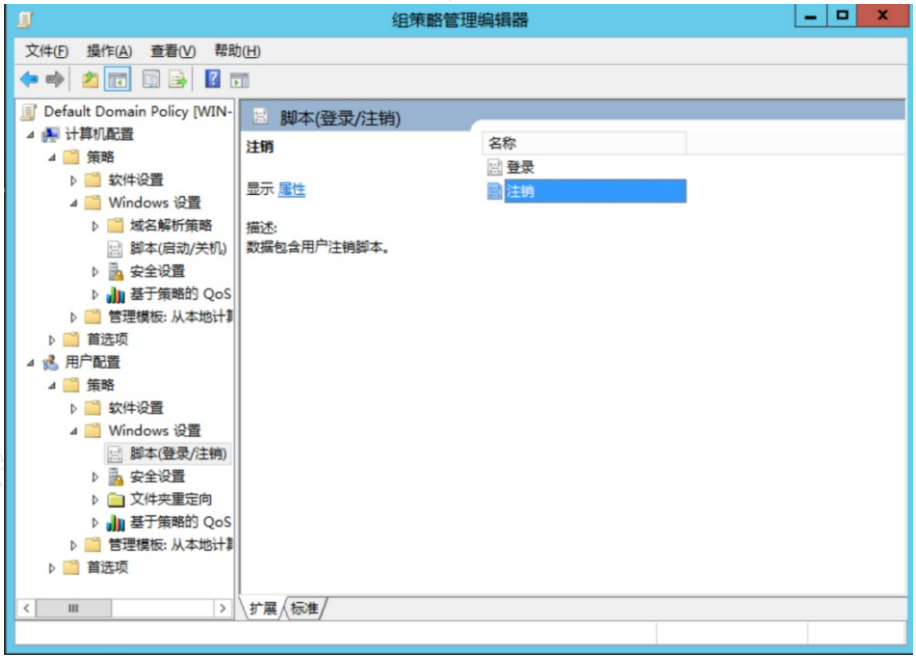


7. 在弹出的登录脚本编辑窗口中单击添加按钮，在添加脚本窗口中，点击<浏览>，选择保存的登录脚本文件(即logon.exe)，并在脚本参数中输入AC的IP，端口号(IPV4支持1773和1775端口，IPV6支持1775端口)，密钥(必须与AC端设置的密码一致)。每个参数以空格分隔，点击<确定>，依次关闭所有组策略属性页面配置。

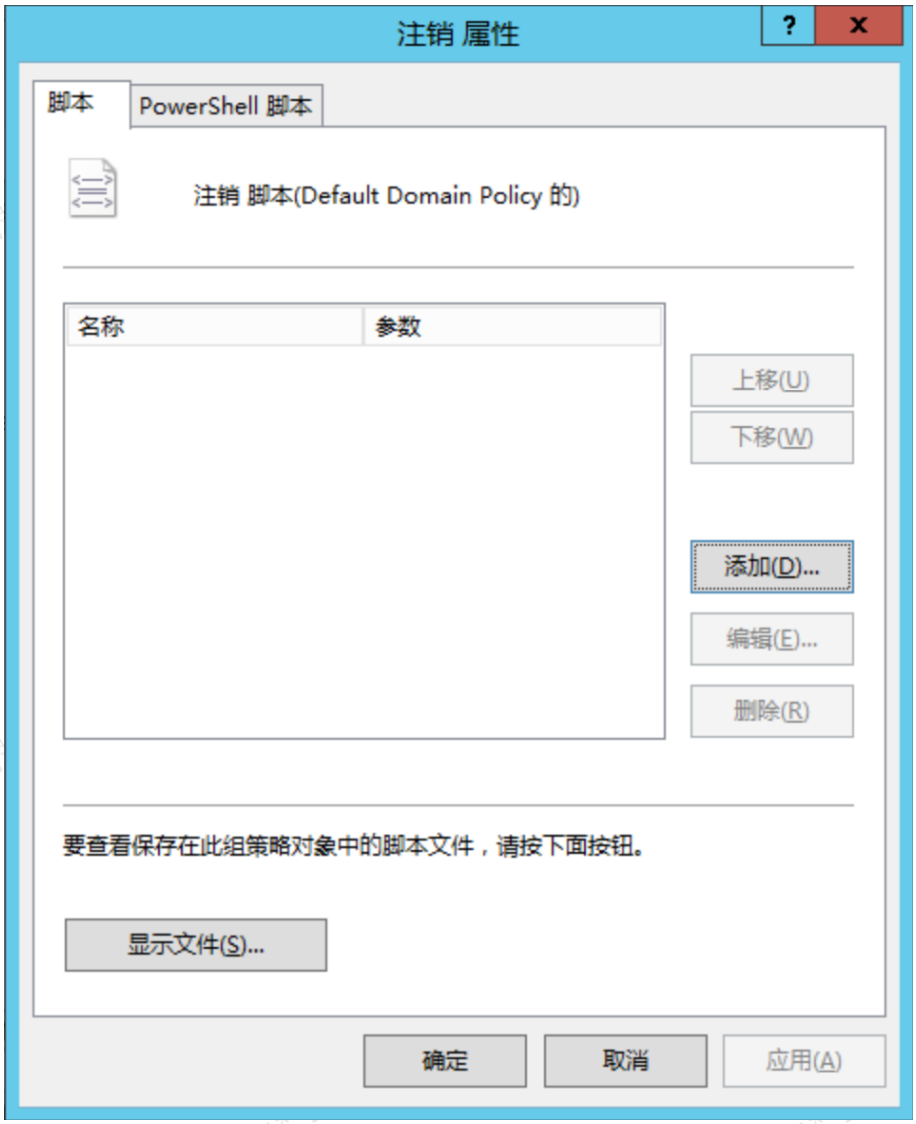


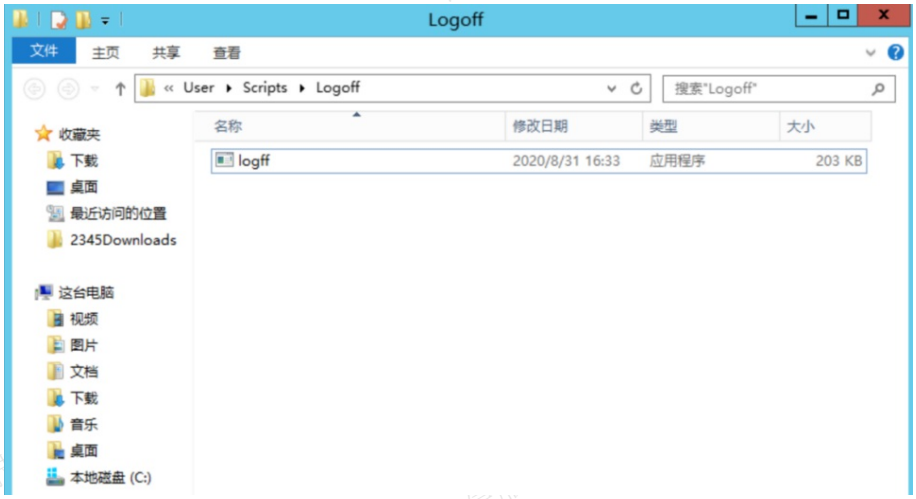
步骤7.在LDAP上配置注销脚本程序。设置注销脚本的目的是在用户注销域的时候同时注销在设备上的登录账号。

1. 在组策略管理编辑器的[用户配置/windows设置/脚本（登录、注销）]，操作配置可参考登录脚本程序的步骤，双击<注销>选项。

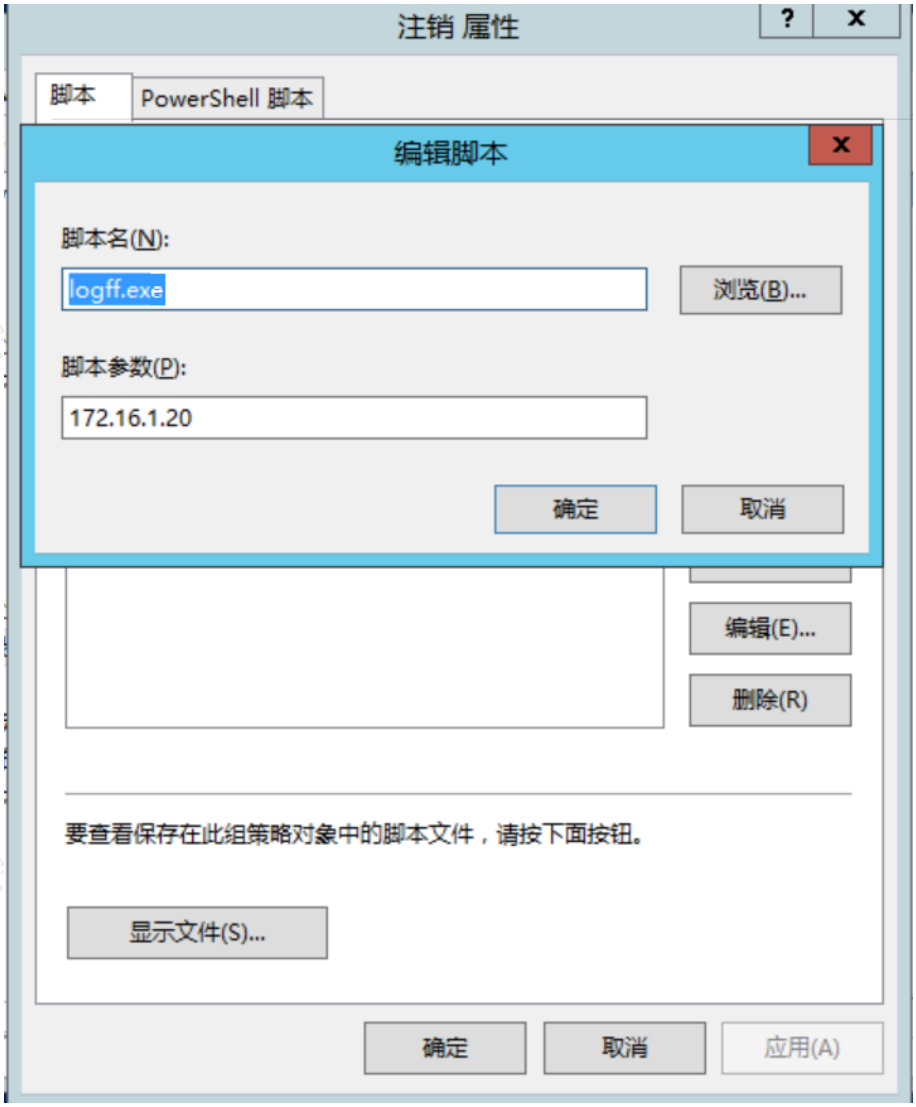


2. 在弹出的注销脚本编辑窗口左下脚点击<显示文件>，将打开一个目录然后将注销脚本(即logff.exe)文件保存在该目录下，关闭该目录。

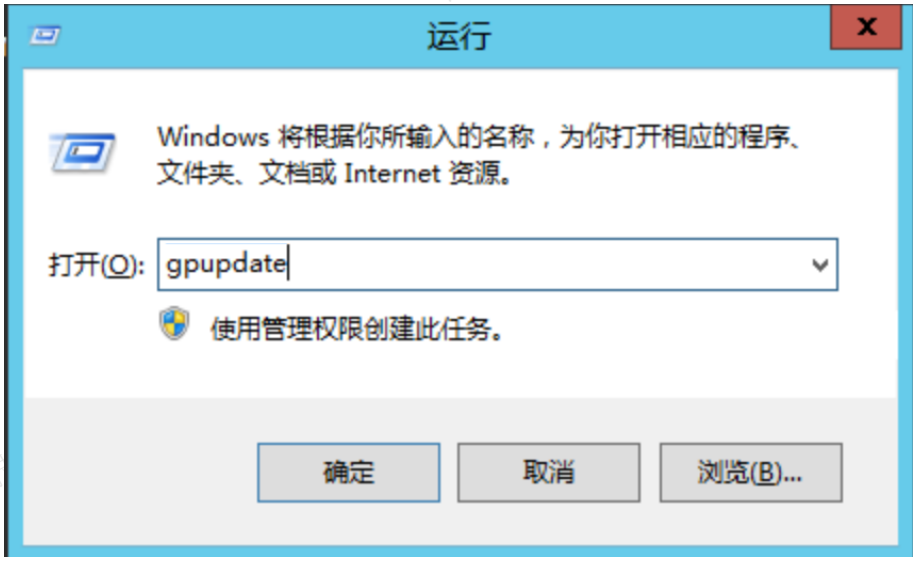




3. 在弹出的注销脚本编辑窗口中单击添加按钮，在添加脚本窗口中，点击<浏览>，选择保存的AD注销脚本文件(即logff.exe)，并在脚本参数中输入在配置注销脚本参数时输入的AC的IP，依次关闭所有的组策略属性页面配置。



4. 配置完脚本后，依次点击桌面左下角的<开始>，点击<运行>，在弹出的运行窗口中输入："gpupdate"并点击<确定>，生效配置完的组策略。



步骤8.用PC登录域，登录域成功后即可在AC上以单点登录方式上线并上网。

说明：

1．要求用户PC的首选DNS填写为域服务器的IP地址，否则会因无法解析域的IP而导致登录不了域服务器。

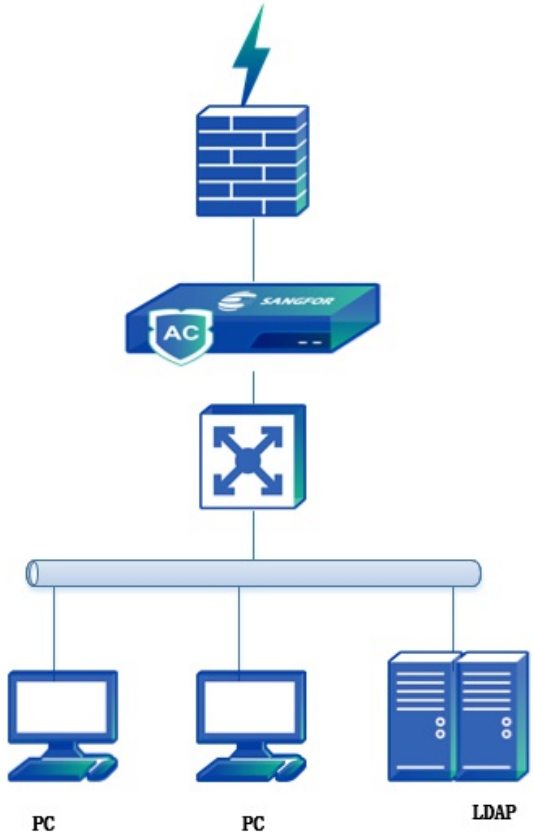
2．如果第一次用户登录域成功后，修改了DNS或者IP地址，此时可以用正确的密码登录到域，可以进入windows，但实际上没有登录到域，此时单点登录无效，用户上网时仍会弹出认证框要求输入用户名和密码，这个主要是因为windows可以记住上次输入的正确密码，没有登录到域也可以进入windows。

3．要求域服务器IP，设备IP以及用户PC能够相互通信。

4．6.x及以前的logon脚本只支持1773端口，11.x以及后面版本的logon支持1775端口(11.x的logon支持IPv4和IPv6)。

通过程序自动获取登录信息（免插件单点登录）

AC设备自带有ADSSO单点登录程序，这个程序可以定期连接AD域，从域服务器上获取PC登录域成功的状态，从而实现单点登录。



数据流过程大致如下：

1. PC登录域。

2. 单点登录客户端程序从LDAP服务器获取成功登录域服务器的用户信息。

3. 获取到用户信息后在AC上自动上线。

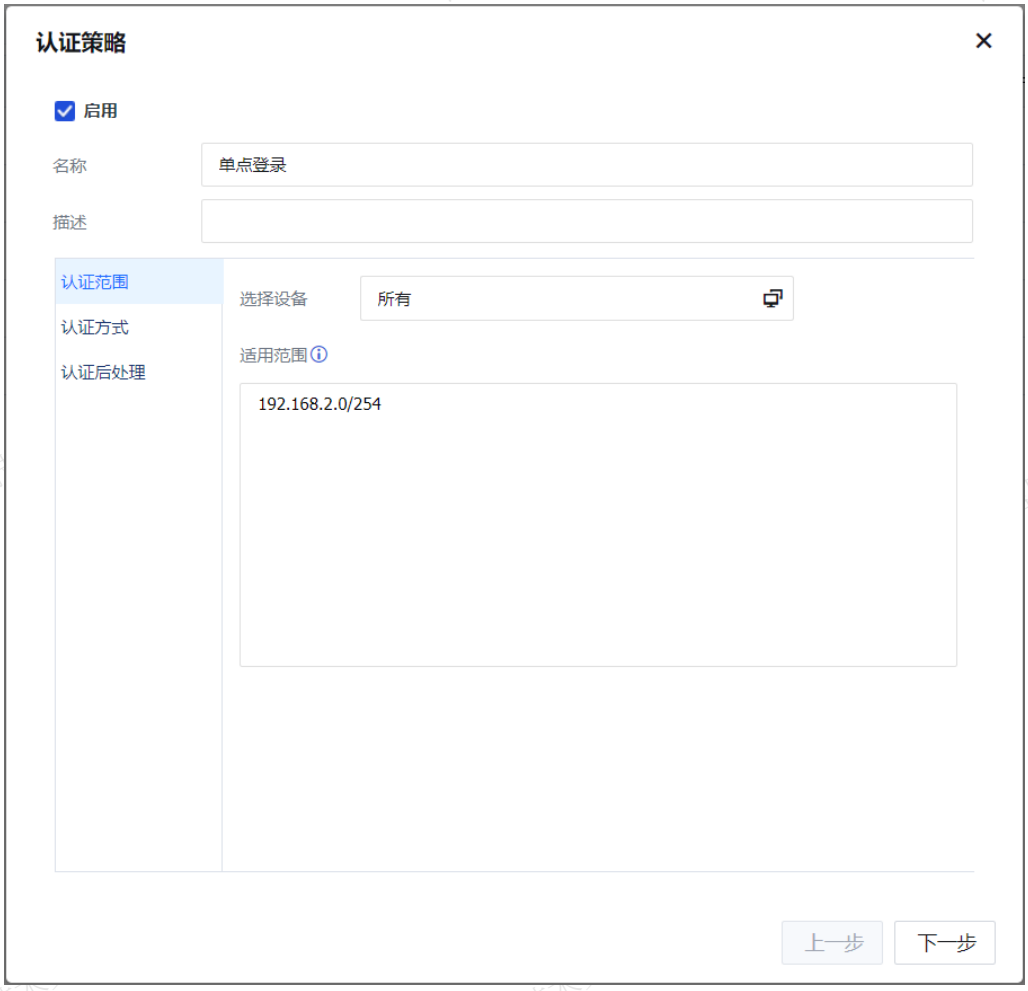
配置案例：要求对内网192.168.2.0/24网段的用户使用AD域单点登录的认证方式，认证成功后通过域账号上线；并且将用户和MAC进行自动绑定（跨三层）；当单点登录失败时用户可以不需要认证上线，以MAC作为用户名，但是只能作为临时用户，以“/限制组/”的权限上网，不能添加到组织结构。

操作步骤

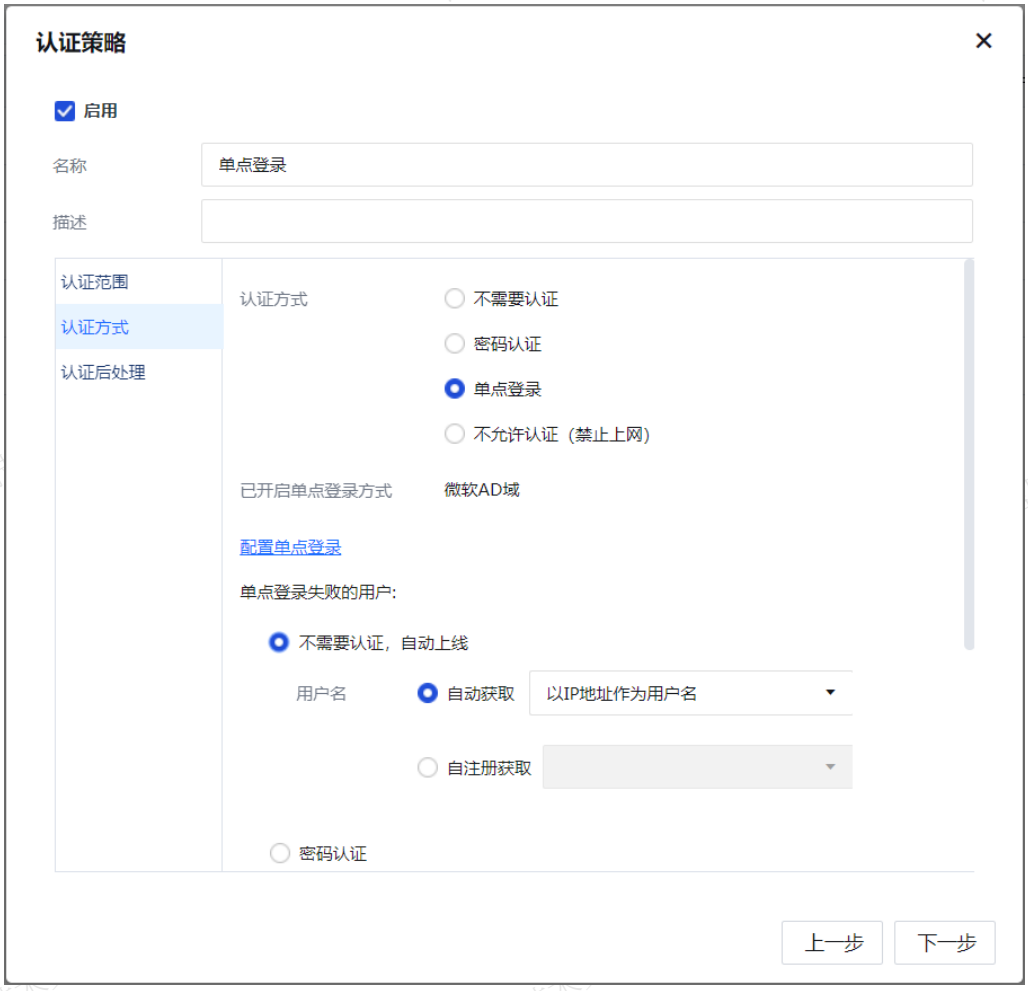
步骤1.设置认证AD域服务器，点击进入[接入管理/接入认证/PORTAL认证/认证服务器]进行设置（参见LDAP服务器章节）。

步骤2.根据需要使用单点登录的用户IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略] 新增认证策略：

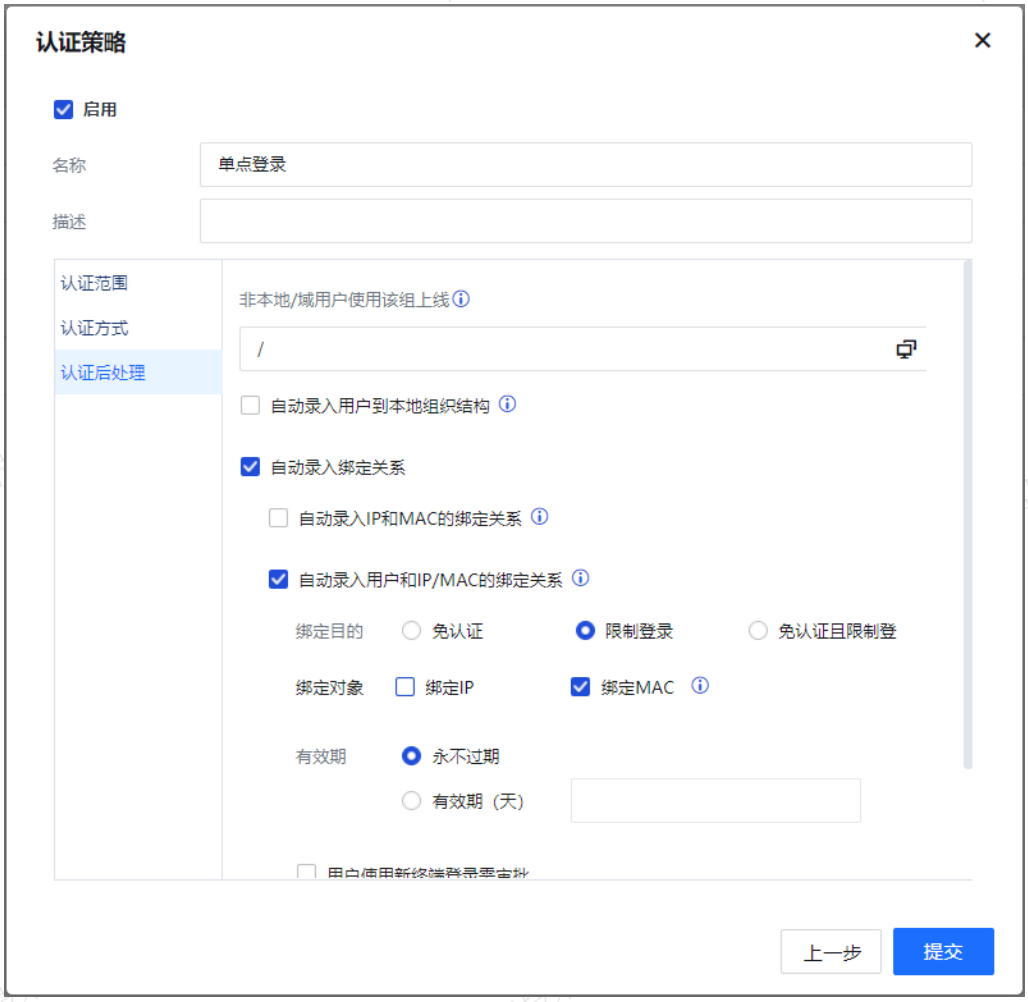
步骤3.设置认证范围，填写适用范围：192.168.2.0/24。



步骤4.设置认证方式，认证方式选择单点登录，勾选不需要认证，自动上线，用户名设置为自动获取：以MAC地址作为用户名。



步骤5.设置认证后处理：勾选自动录入绑定关系：绑定目的选择：限制登录，绑定对象选择绑定MAC，有效期：设置为永不过期。



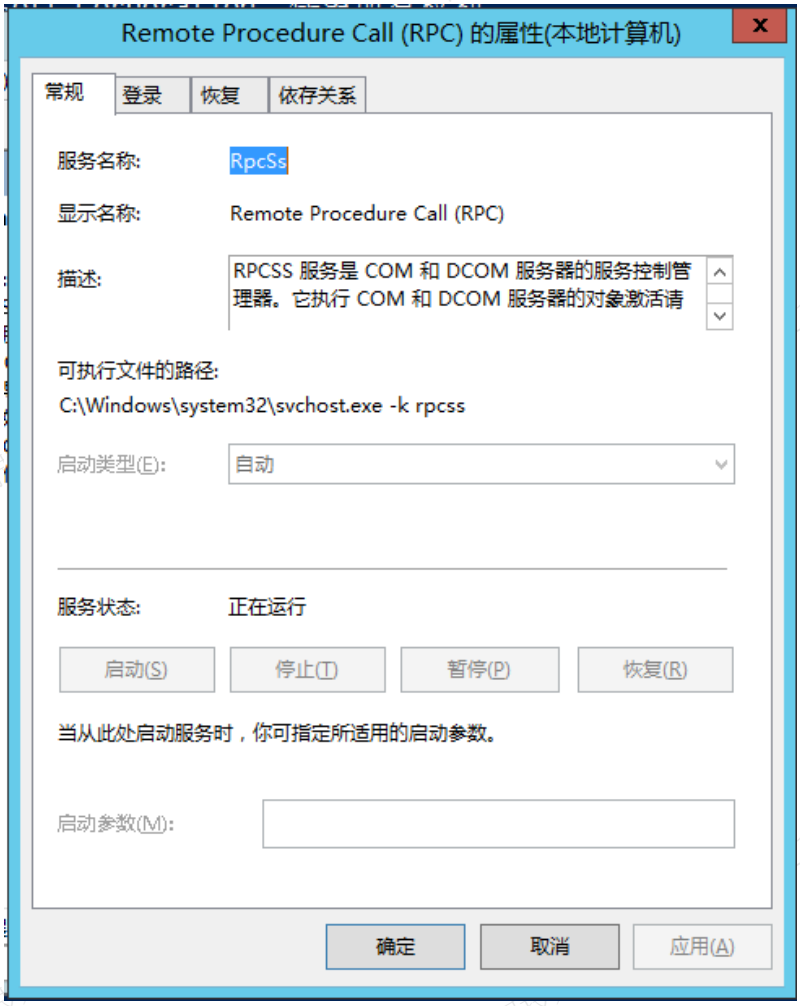
步骤6.因为用户环境是跨三层环境，同时需要绑定MAC地址，需要配置跨三层取MAC的功能，在[接入管理/接入认证/PORTAL认证/认证高级选项/跨三层取MAC]页面进行配置。参考SNMP章节。

步骤7.在设备上启用单点登录。在[接入管理/接入认证/PORTAL认证/单点登录/微软AD域]页面勾选[启用域单点登录]和[域监控单点登录]。

步骤8.点击<新增>，添加AD域服务器，设置域服务器的IP地址。

步骤9.检查和确认AD域服务器的相关配置是否已经启用。

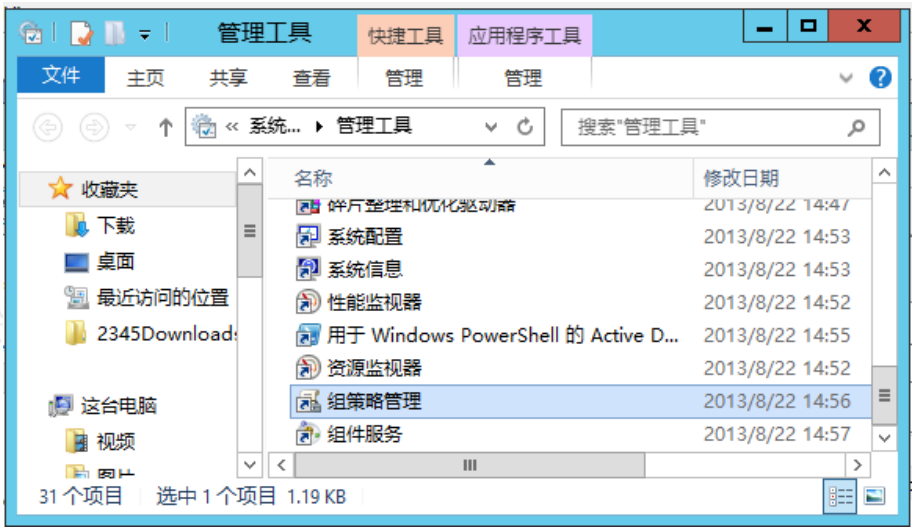
步骤10.确保AD域服务器上的RPC远程调用服务正常启用运行，在[任务管理器/服务]找到Remote Procedure CALL(RPC)服务，点击<启用>。



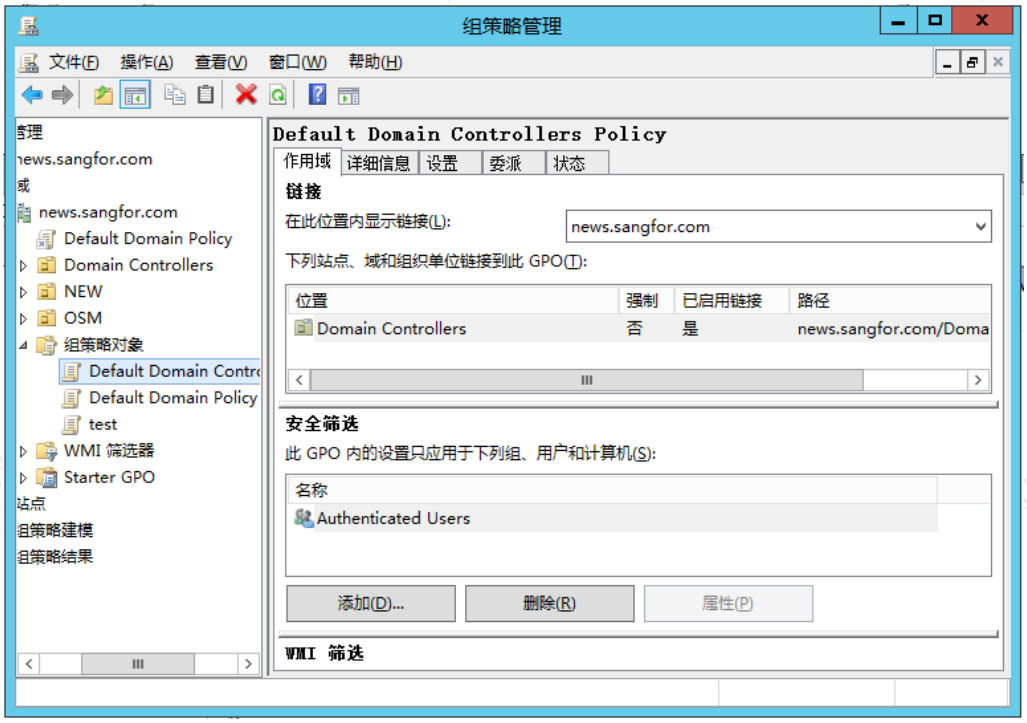
步骤11.Eventlog方式获取用户的配置：

1)开启AD 域的Eventlog 审计。

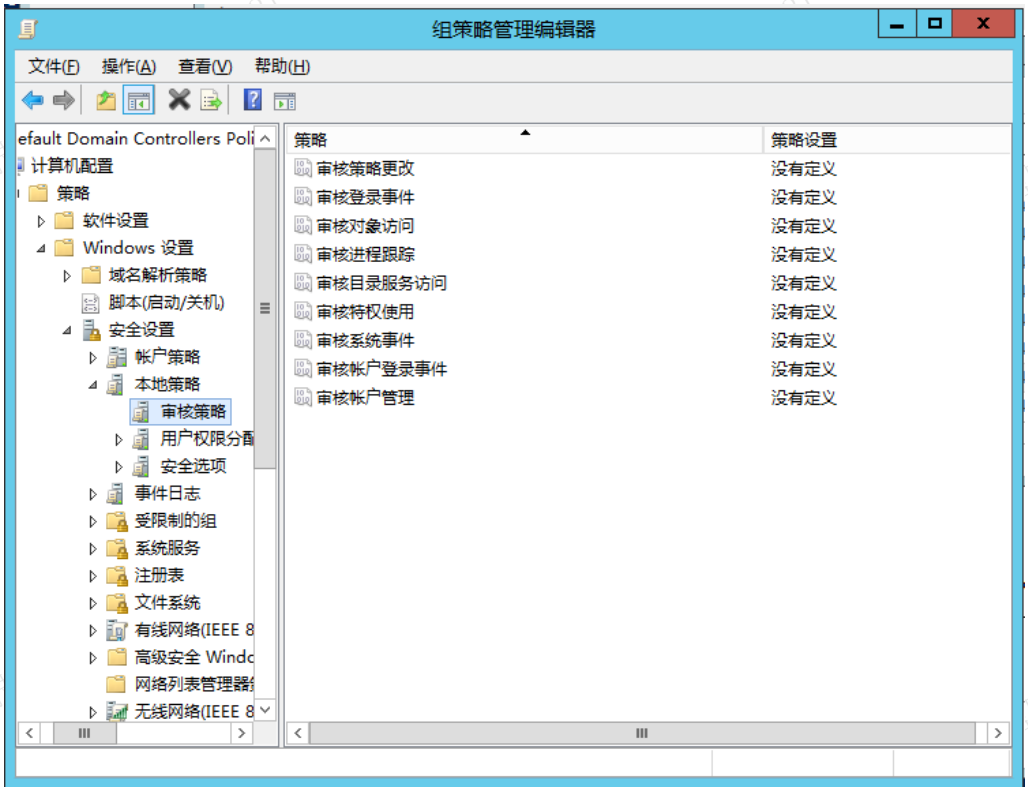
2)在AD域服务器中进入[控制面板/系统和安全/管理工具]页面。



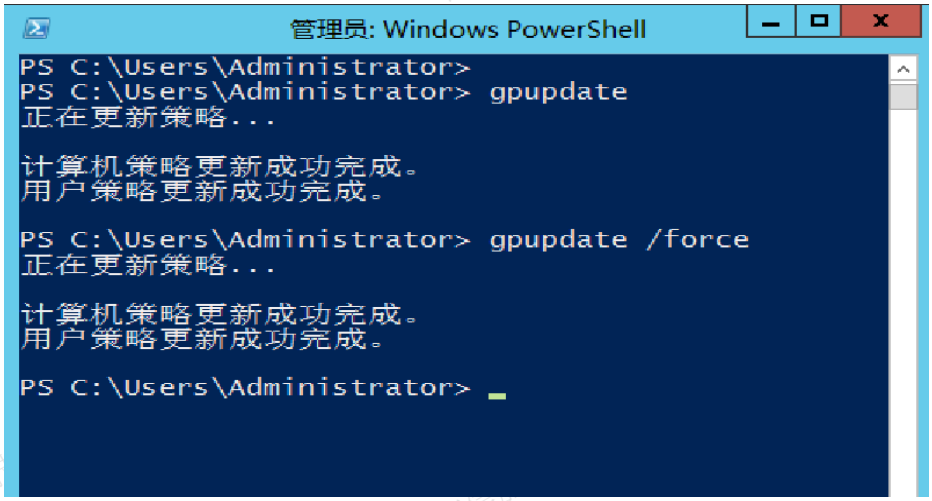
3)点击<组策略管控>页面编辑“Default Domain Controllers Policy”。



4)在计算机配置的[策略/域名解析策略/安全设置/审核策略]中，开启“审核登录事件”和“审核账户登录事件”。



5)使用WIN+R在运行中输入cmd运行窗口，输入“gpupdate”“gpupdate / force” 刷新策略。



使用集成Windows身份认证方式实现单点登录

通过在AC设备上开启集成Windows身份认证功能，AC设备和内网电脑都加入到AD域。内网用户成功登录域并访问网页，即可在AC设备上自动通过认证。

操作步骤

步骤1.设置认证AD域服务器，点击进入[接入管理/接入认证/PORTAL认证/认证服务器]进行设置（参见LDAP服务器章节）。

步骤2.根据需要使用单点登录的用户IP或MAC设置认证策略，在[接入管理/接入认证/PORTAL认证/认证策略/]新增认证策略。

步骤3.AC设备启用单点登录。在[接入管理/接入认证/PORTAL认证/单点登录/微软AD域]页面勾选[启用域单点登录]和[启用集成Windows身份验证]，设置域服务器的IP地址。

步骤4.点击测试有效性，会显示测试结果。

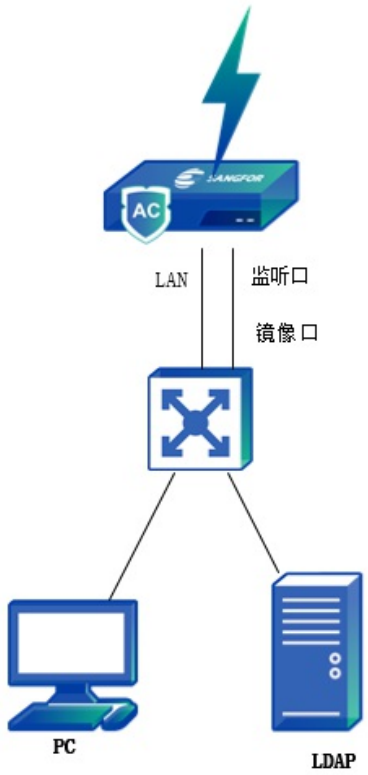
步骤5.点击<提交>，保存和生效配置，大概一分钟左右，右下角小喇叭会有提示是否加入域成功。

步骤6.成功登录域后的PC打开网页，查看AC设备的在线用户列表，即可显示认证成功的用户。

使用监听模式实现单点登录

监听模式是通过监听PC登录域服务器的数据，从监听到的数据中获取用户登录的信息，从而实现的单点登录。监听模式的单点登录无需在域服务器上安装任何组件，但要求内网电脑登录域的数据经过设备或者是通过监听口镜像到设备。设备通过监听UDP 88端口的登录信息，如果用户成功登录域，则上网时无需再次通过我们设备的认证，可以直接上网。适用于域服务器在外网和内网情况。下面分两种情况介绍单点登录的设置。

第一种情况：域服务器在内网环境：



数据流过程如下：

1. PC登录域的数据不经过AC，在内网转发；

2. 在交换机上设置镜像口，把PC登录域的数据镜像到AC上；

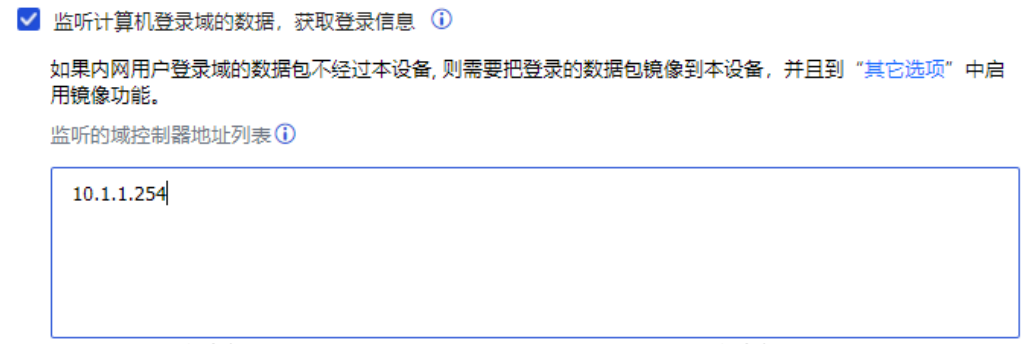
3. 如果用户登录域成功，则自动通过设备认证。

操作步骤

步骤1.设置认证AD域服务器，点击进入[接入管理/接入认证/PORTAL认证/认证服务器]进行设置（参见LDAP服务器章节）。

步骤2.根据需要使用单点登录的用户IP或MAC设置认证策略，在[PORTAL认证/认证策略] 新增认证策略。

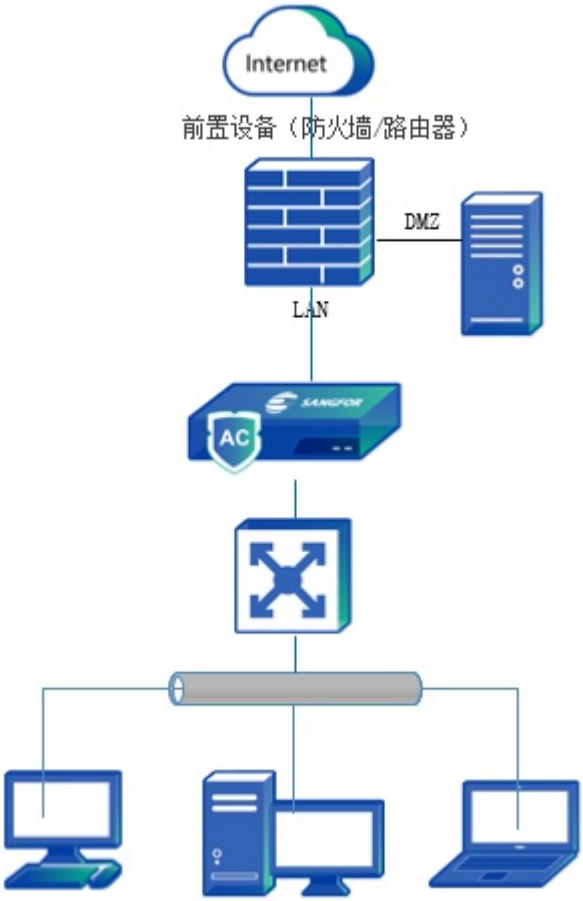
步骤3.AC设备启用单点登录。在[接入管理/接入认证/PORTAL认证/单点登录/微软AD域]页面勾选[启用域单点登录] 和[监听计算机登录域的数据，获取登录信息]，表示使用监听模式实现单点登录。在[监听的域控制器地址列表]中输入域服务器的IP和监听端口，如果有多个域服务器，则一行一个IP和端口，如下图所示。



步骤4.这种部署中，内网登录域服务器的数据不经过设备，需要通过设置镜像口，并将镜像口连接到转发登录数据的交换机镜像口上，点击<其它选项>，设置设备的镜像口。镜像口需要设置空闲网口，已经在使用的网口请不要设置成镜像网口。

步骤5.PC登录域，登录成功后即可上网。

第二种情况：域服务器在外



数据流过程如下：

1. PC登录域是穿透设备的；

2. 设备的内网接口同时作为监听口，无需再设置监听口。

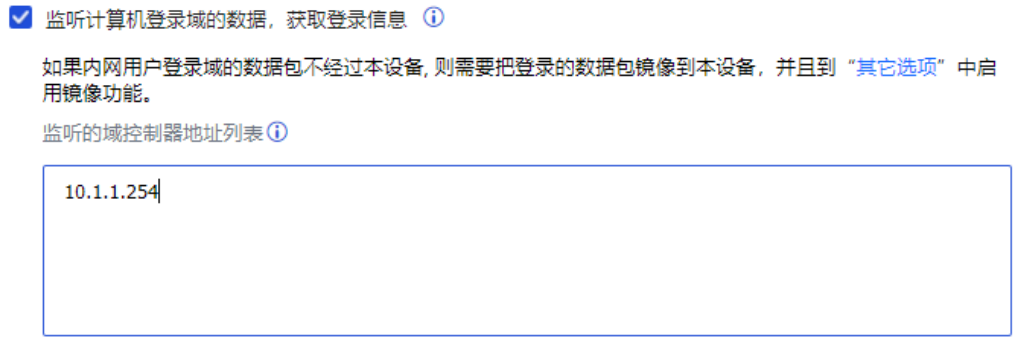
操作步骤

步骤1.设置认证AD域服务器，点击进入[接入管理/接入认证/PORTAL认证/认证服务器]进行设置（参见LDAP服务器章节）。

步骤2.根据需要使用单点登录的用户IP或MAC设置认证策略，在 [接入管理/接入认证/PORTAL认证/认证策略] 新增认证策略。

步骤3.因为LDAP服务器在设备的外网方向，用户认证前需要放通访问域服务器的权限，在[认证策略/认证后处理/高级选项/认证前使用此组权限]中设置一个认证前使用的组，并在上网策略中放通这个组访问域服务器的权限。

步骤4.AC设备启用单点登录。在[接入管理/接入认证/PORTAL认证/单点登录/微软AD域]页面勾选[启用域单点登录]，勾选[监听计算机登录域的数据，获取登录信息]，表示使用监听模式实现单点登录。在[监听的域控制器地址列表]中输入域服务器的IP和监听端口，如果有多个域服务器，则一行一个IP和端口。



步骤5.PC登录域，登录成功后即可上网。

说明：

监听模式只能监听到用户登录的信息，用户注销时没有数据，故无法监听到注销的状态，所以可能会出现PC已经注销了，但设备的在线用户列表中还没有注销此用户。

终端管理

终端检查主要功能是对用户接入终端后进行安全性检查和控制终端的行为。

安全性检查目前支持杀软检查、登录域检查、操作系统检查、进程检查、文件检查、注册表检查、计划任务规则、补丁检查、软件检查等检查规则，检查完之后支持按照检查结果控制访问。

控制场景包括外联控制、外设管控等，检查终端是否存在未授权的连接外网行为，如果检测到存在违规，则禁止终端网卡实现访问控制，包括拨号检查，无线网卡检查，连接外网检查等。

配置流程

管理员需要配置终端检查策略的思路：

1. 在[接入管理/终端管理/终端检查规则]，配置需要检查的规则。
2. 配置检查策略，包括策略名称（必填）、描述信息（可不填），检查策略选择终端插件检查或者流量行为检查，设置适应对象和高级配置。
3. 配置违规后的处置。

检查策略

检查策略的作用是对所有终端的合规性和非法外联做检查和管控，策略的配置先根据检查规则的设置而进行自定义，以下是检查策略配置的步骤。

操作步骤

步骤1.配置完成检查规则设置之后，在导航菜单中的[接入管理/终端管理/终端检查策略]里新建一条策略，点击启用该策略，输入策略名称和描述信息。

步骤2.在策略设置有终端插件检查和流量行为检查可选，勾选相应的已经配置好的检查规则，点击<添加>。选择之前创建的规则的类型，生效时间按需选择，然后点击<确定>。

步骤3.在[适用对象]页面选择该策略生效的用户，可以根据用户、位置、终端类型、目标区域选择需要检查的对象。

步骤4.在[高级配置]页面可设置该策略过期时间、同级别管理员查看编辑权限设置、是否允许低级别管理员查看。

步骤5.点击<提交>，至此完成检查策略功能配置。

检查策略管理

在管理员对所有的检查策略进行删除操作、批量编辑、启用和禁用、导入/导出、上移/下移等操作，还可以进行过滤选择。

检查策略管理功能说明

操作	功能说明
删除策略	检查策略列表页面，可点击删除相应的策略。
编辑/批量编辑	在检查策略列表页面，勾选需要编辑的检查策略，点击检查策略名称，设备会弹出检查策略的编辑页面，修改选中策略的相关信息。 批量编辑：勾选多个自定义的检查策略，可编辑策略的适用对象，其他信息不可以修改。
导入/导出	支持检查策略的导入/导出，选中自定义的策略然后勾选相应的策略，点击导出，即可将选中的策略导出，注意：内置的检查策略无法导出。点击导入，选中需要导入的检查规则文件，即可进行导入。
启用/禁用	选中已禁用的策略，点击启用，该策略即可生效，选中已启用的策略，点击禁用，该策略会失效。
上移/下移/移动到	由于策略是自上而下进行匹配，所以可以选中相应的策略，点击上移或者下移，或自定义移动，来进行优先匹配策略。
过滤	可输入需要过滤策略的名称，进行策略的过滤。

检查规则

检查规则主要分为终端插件检查规则和流量行为检查规则。实现终端插件检查规则时，终端需要安装准入插件，流量行为检测规则是通过检查流量实现，终端无需安装准入插件。

终端插件检查规则

第一步：在[接入管理/终端管理/终端检查规则/插件检查规则]，点击<新增>需要配置的检查规则。

第二步：填写规则名称和规则描述，规则类型可选中菜单里的规则类型，也可以直接在对话框内输入自定义的规则类型名称选择检查项配置，根据配置的检查规则选择需要检查的项，如下表可选。

说明

当配置检查策略时，添加的规则类型就是在检查规则的类型输入的名称，因此建议规则类型需要填写跟该规则匹配，以便后续调用。

终端插件检查规则

表12终端插件检查规则检查项表

规则名称	检查项说明
杀软检查	检查的杀毒软件主要包括360杀毒、瑞星杀毒、金山毒霸、腾讯电脑管家、2345安全卫士、瑞星个人防火墙、小红伞、卡巴斯基、Avast、赛门铁克(SEP)、趋势杀毒软、诺顿杀毒软件、McAfee(MSC)、Windows Defender 微软杀毒、江民杀毒 、熊猫卫士、火绒互联网安全、大蜘蛛杀毒软件等。
登录域检查	必须登录到域；需要登录到指定域：可以自定义。
操作系统检查	Windows XP、Windows2003、Windows7、Windows8、Windows10、Windows11、Windows2012R2、Windows2016、Windows Vista、Windows2008R2 Windows2008的部分操作系统，也可以根据版本进行选择。
进程规则	进程名称、窗口名称、程序路径。 进程状态：正在运行和没有运行。 高级条件：可设置匹配程序MD5值和匹配程序大小。
文件规则	文件路径：存放的路径。 文件状态：文件存在和文件不存在。 高级条件：设置匹配文件的MD5值、文件大小、更新日期比当前日期滞后的天数。
注册表规则	注册表项、表项名称、表项数据。 表项状态：有和没有。
	执行程序 1. 输入程序路径或点击上传文件。 2. 配置程序运行所需参数，与上面程序搭配使用。

计划任务规则	**执行计划** 检查项说明 1. 连续运行：最小时间间隔为40秒。 2. 运行一次：计算机上准入程序启动时运行。
	执行权限 3. 当前用户执行权限。 4. 以SYSTEM用户权限执。
	结果检查 5. 不检检查返回结果。 6. 检查返回结果。
补丁检测规则	按指定级别检测；按指定补丁检测；获取pc补丁信息识别时按违规处理
外联检查规则	拨号行为、有无线网口、双网卡行为、有4g网卡、连接外网、自定义外联、连接非法WIFI、使用非法网关。
外联控制规则	只能访问以下地址；不能访问以下地址。
外设管控规则	**禁止使用的外设类型** 存储设备、网络设备、蓝牙设备、摄像头、打印机。 **精细化管控** U盘及移动硬盘接入：可读写、拒绝、可读、告警。 便携设备接入：允许、禁用、告警。
Windows规则	禁止以计算机的超级管理员（隶属于Administrators组的帐户）身份登录计算机，否则禁止该计算机上网。

防规避则改名检查规则	**检查项说明** 可设置不能修改MAC或IP。
客户端集成规则	All in one场景联动EDR、atrust推端。启用该规则时，需完成“终端安全联动”配置。
软件检查规则	通过准入客户端检查终端的注册表信息，获取终端当前软件安装列表，并根据配置的软件检查规则判断当前客户端是否存在违规情况，如存在违规，则根据软件检查规则配置的违规处置动作，对客户端进行处置。 **判定方式** 7. 如果已安装下列任意一款软件，视为违规。 8. 如果已安装下列任意一款软件，视为合规。 9. 如果安装下列所有软件，视为合规。
桌面水印管控规则	为Windows桌面添加水印标识
端口管控规则	放通以下端口；封堵以下端口
应用联网管控规则	对指定应用联网权限进行控制，包括：禁止联网；允许联网；仅禁止访问以下地址；仅允许访问以下地址。

规则名称	检查项说明
说明	

操作系统检查：补丁包对Windows XP要求是SP2或以上，windows10可选择版本和无要求。

文件检查：规则只使用于同时配置条件的文件。

补丁包检测：该规则不支持Windows xp、Windows Server2003及其以下的操作系统版本；同时勾选按指定级别检测和按指定补丁检测时，其中任何一种方式检测出违规即为违规。

外联检查规则：其中连接非法WIFI和非法网关有白名单设置。

外设管控规则：windows xp系统和全线的家庭版系统没有组策略，不支持组策略的管控方式；精细化管控只支持win7及以上版本，不区分是否家庭版；精细化管控只针对usb接口的存储设备(U盘移动硬盘便携设备)。

软件检查规则：通过绿色安装的软件无法监测，即注册表没有信息的。

桌面水印管控规则：用户名包含emoji，如水印规则勾选了用户名，则水印可能存在乱码。首次下发水印检查策略，终端需要从AC设备获取水印组件，需要等待3分钟左右才会生效。

终端插件检查后违规处置

表13终端插件检查规则违规处置表

检查规则	违规处置
杀软检查	包括：禁止上网并提示用户、提示用户、违规修复、限制用户权限、自定义提示内容。
登录域检查规则	包括：禁止上网并提示用户、提示用户、只记录结果、限制用户权限、自定义提示内容。
操作系统规则	包括：禁止上网并提示用户、提示用户、只记录结果、自定义提示内容。
进程规则	包括：禁止上网并提示用户、停止进程、提示用户、只记录结果、自定义提示内容。
文件检查	包括：禁止上网并提示用户、删除文件、提示用户、只记录结果、自定义提示内容。
计划性任务规则	包括：禁止上网并提示用户、删除该项、提示用户、只记录结果、自定义提示内容。
注册表规则	包括：禁止上网并提示用户、提示用户、只记录结果。
补丁检测规则	包括：提示用户、只记录结果。

外联检查规则	包括：发送告警邮件、断网、自定义提示内容。
外设管控规则	包括：白名单设置，可讲对应设备应将ID加入到白名单中。
防篡改检查规则	包括：禁止上网并提示用户、恢复修改前地址并提示用户、提示用户、只记录结果。其中选择不能修改IP违规处置只能选择恢复修改修改前地址并提示用户。
软件检查规则	包括：只记录结果、安装指定软件、提示用户、禁止上网并提示用户。 其中判定方式为[如果已安装下列任意一款软件，视为合规]和[如果安装下列所有软件，视为合规]时才支持“安装指定软件”。
桌面水印管控规则	**控制项配置** 水印显示内容：包括用户名、时间、用户显示名、部门/组、IP地址、Mac地址、Windows登录名、计算机名，至少选择一项。 自定义内容：可自定义显示水印内容（可选）。 水印透明度：可配置水印透明度范围，默认值20。 水印密度：高、中、低，默认值中。

第三步：配置违规后处置，根据不同的检查规则，选择相应的违规处置。点击<提交>检查规则即可配置完成。

组合规则

第一步：在[接入管理/终端管理/终端检查规则/插件检查规则]，点击<组合规则>，点击<新增>一条组合规则。

第二步：填写规则名称和规则描述，规则类型可选中菜单里的规则类型，也可以直接在对话框内输入自定义的规则类型名称，该规则类型用于后续新增规则策略时调用。组合规则成立可选：所有规则成立和任意一个规则成立。

第三步：组合规则设定在待选规则里选中需要设置的规则，点击<添加>会添加到已选的规则中，如待选列表没有规则可选，在终端插件检查规则创建操作系统规则、进程规则、文件规则、注册表规则、计划任务规则、补丁包检测规则、windows账号规则。

第四步：违规后操作：禁止上网或提示用户、提示用户、只记录结果。也可以点击<编辑提示内容>自定义提示内容。

第五步：点击<提交>，组合规则配置完成。

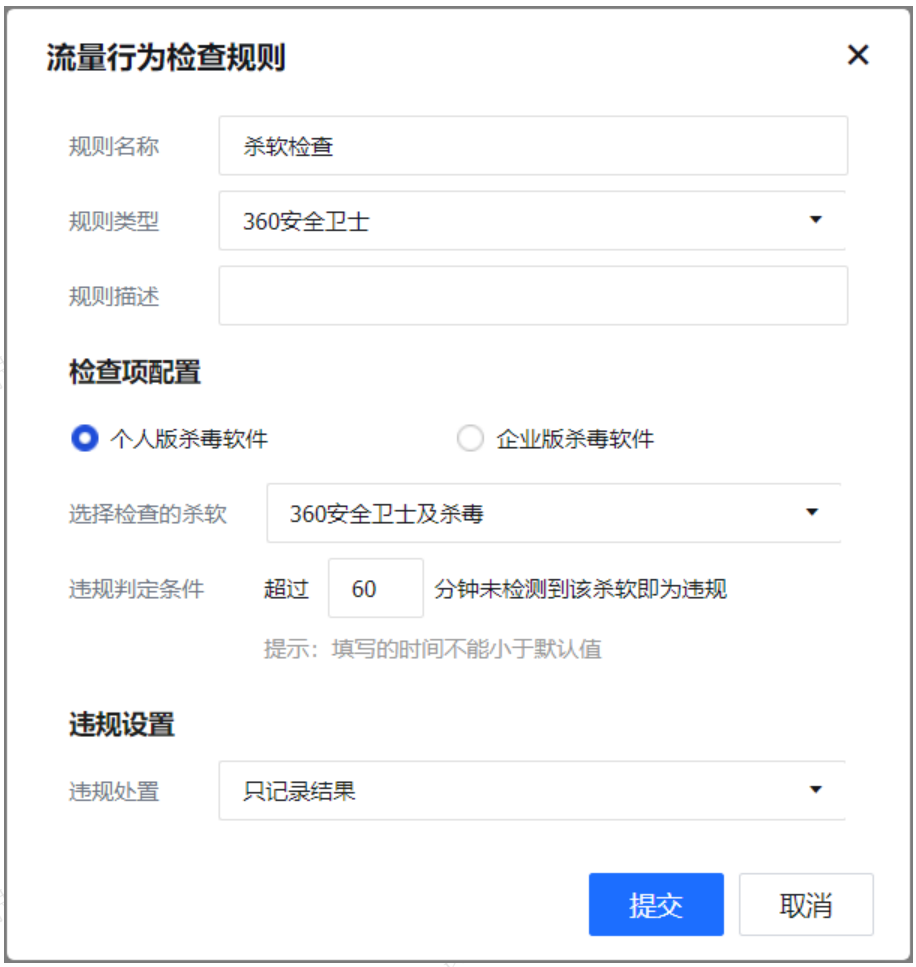
说明：

组合规则功能只支持：操作系统规则、进程规则、文件规则、注册表规则、计划任务规则、补丁包检测规则、Windows账号规则。其他规则暂时不支持组合操作。

流量行为检查规则

第一步：在[接入管理/终端管理/终端检查规则/流量检查规则]，点击<新增>需要配置的检查规则。

第二步：填写规则名称和规则描述，规则类型可选中菜单里的规则类型，也可以直接在对话框内输入自定义的规则类型名称。



第三步：检查项配置可选个人版杀毒软件或企业版杀毒软件。个人版杀毒软件是设备已定义流量特征，企业版杀毒软都会有指定服务器地址，通过检查终端是否有流量来判断是否安装杀毒软件。

个人版杀毒软件

可选择检查的杀软有：360安全卫士以及杀毒、金山毒霸、火绒安全软件、腾讯电脑管家、小红伞、卡巴斯基、赛门铁克。

违规判定条件：根据不同的杀毒软件设置的默认时间进行检测是否有该杀软，填写时间不能小于默认值。

企业版杀毒软件

可选择检测的杀软有：EDR、360天擎、卡巴斯基、赛门铁克、自定义企业杀软。

违规判定条件：需要根据企业版杀软配置的更新频率来设置，（EDR默认超过1分钟未检测到该杀软即为违规，建议配置为5分钟），每个应用都有不同的最小默认值，用户配置必须大于默认值。

第四步：设置违规后处置可选择：只记录结果或定期重定向至指定网址修复，选择定期重定向至指定网址修复，需要配置重定向配置：重定向网址和重定向间隔时间。

第五步：点击<提交>，流量检测规则配置完成。

检查规则管理

在[接入管理/终端管理/终端检查规则]，管理员对终端插件检查规则和流量行为检查规则进行删除操作、批量编辑、导入/导出等操作，组合规则仅支持删除和编辑操作。

表14检查规则管理功能说明

操作	功能说明
删除	在检查规则页面，选择终端插件检查规则、组合规则、流量行为检查规则，勾选需要删除，点击删除，设备会弹出一个操作确认框，点击<是>，则删除选中的规则。
编辑	在检查规则页面，选择[终端插件检查规则、组合规则、流量行为检查规则，勾选需要编辑的检查规则，点击检查规则名称，设备会弹出检查规则的编辑页面，修改检查策略，除了规则名称无法修改，其他设置项均可以进行修改。
批量编辑	批量编辑检查规则：勾选多个自定义的检查规则，可以批量修改检查规则的类型，点击批量编辑，则弹出[批量编辑]页面。注意批量编辑只能编辑检查规则的类型。
导入/导出	检查规则支持规则的导入导出，在[检查规则]页面，选择终端插件检查规则、流量行为检查规则然后勾选相应的规则，点击导出，即可将选中的规则导出，

说明：

1．当已经被检查策略引用的规则，不能直接删除；如需要删除，需要先删除检查策略中引用到的规则。

2．内置的检查规则无法导出。

3．导入的规则文件一定要是zip格式的，而且导入的文件一定要包含IngressRuleExport.conf文件，IngressRuleExport.conf文件一定要在最外层。

准入客户端配置

准入客户端配置是用来设置设备准入的相关参数，包括认证准入客户端的配置、准入客户端推送配置、准入客户端下载、准入规则排除等。该功能在终端检查策略中会引用此处的配置。

准入客户端功能配置

• 准入客户端认证方式有两种方式：开启准入客户端802.1X功能和开启准入认证客户端Portal认证功能（可选是否开启自动上线功能），这两种认准入方式在接入认证章节的时候根据配置的认证策略进行勾选。

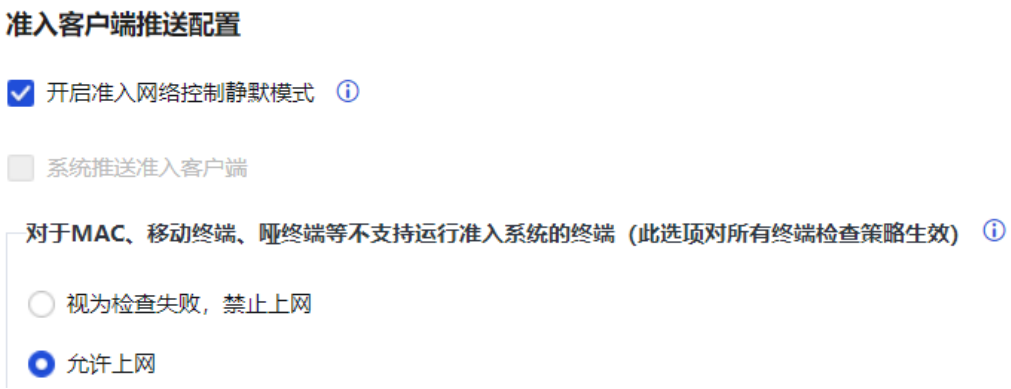
• 设置准入客户端卸载密码：勾选该项可开启插件防卸载功能，卸载插件需要输入密码才能完成卸载，需要终端成功获取检查策略之后防卸载才生效。

• 设置准入客户端找网关地址方式：自动找网关和设置准入客户端网关地址。

说明：

设备在旁路模式下设备会自动找IP，建议勾选“设置准入客户端网关地址”，手动填写网关地址。

系统推送准入客户端



勾选[系统推送准入客户端]后设备会对匹配准入策略但未安装准入客户端的终端推送准入客户端安装界面，同时阻断该类终端的网络访问。不勾选非windows终端不会推送，需要用户手动安装或者通过第三方设备推送。

开启准入网络控制静默模式：勾选后设备将不再执行准入策略的断网动作，只会执行提醒动作。（网络层面

的断网，准入客户端执行的断网动作依然生效）

仅对于MAC、移动终端、哑终端等不支持运行准入系统的终端（此选项对所有终端都生效）。

• 视为检查失败，禁止上网：勾选后对于不安装准入客户端的终端，禁止该终端上网。

• 允许上网：勾选后允许MAC、移动终端、哑终端等不支持运行准入系统的终端正常访问网络。

准入客户端下载

更新准入客户端功能配置后请先点击<提交>再进行下载。

说明：

1、准入客户端防卸载需要结合[接入管理/准入客户端配置]中的<设置准入客户端卸载密码>使用。、

2、在PC安装准入客户端时，需要用户接收用户协议才能完成准入客户端的安装。管理员可点击<查看用户协议>查阅协议相关内容。

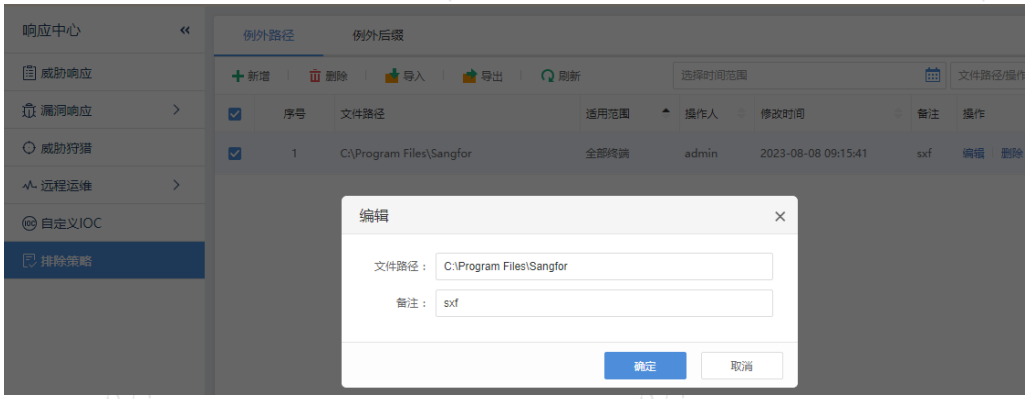
补丁规则排除

忽略补丁检查规则按指定级别检测出来的补丁，不进行提示和网络控制。

准入客户端加入白名单

为了避免终端安全软件（如杀软、桌管等）由于病毒查杀可能带来的误报，导致准入客户端目录文件被删除，从而造成客户端运行故障。建议提前收集终端PC已安装的终端安全软件，并将准入客户端目录：C:\Program Files\Sangfor\ 加入白名单，确保信任目录下的文件不会进行病毒扫描查杀。

以深信服终端安全管理系统EDR为例，登录EDR管理端，在[响应中心/排除策略]例外路径页面中新增排除目录，如下图：



终端检查案例

用户接入认证完成后进行终端安全性检查，目前支持杀毒软件检查、操作系统检查、进程检查、文件检查、注册表检查、计划任务规则、补丁检查等检查规则，检查完之后支持按照检查结果控制访问。如下举例操作系统场景案例，其他配置请参考文档《深信服全网行为管理准入功能配置指导》

链接地址：https://bbs.sangfor.com.cn

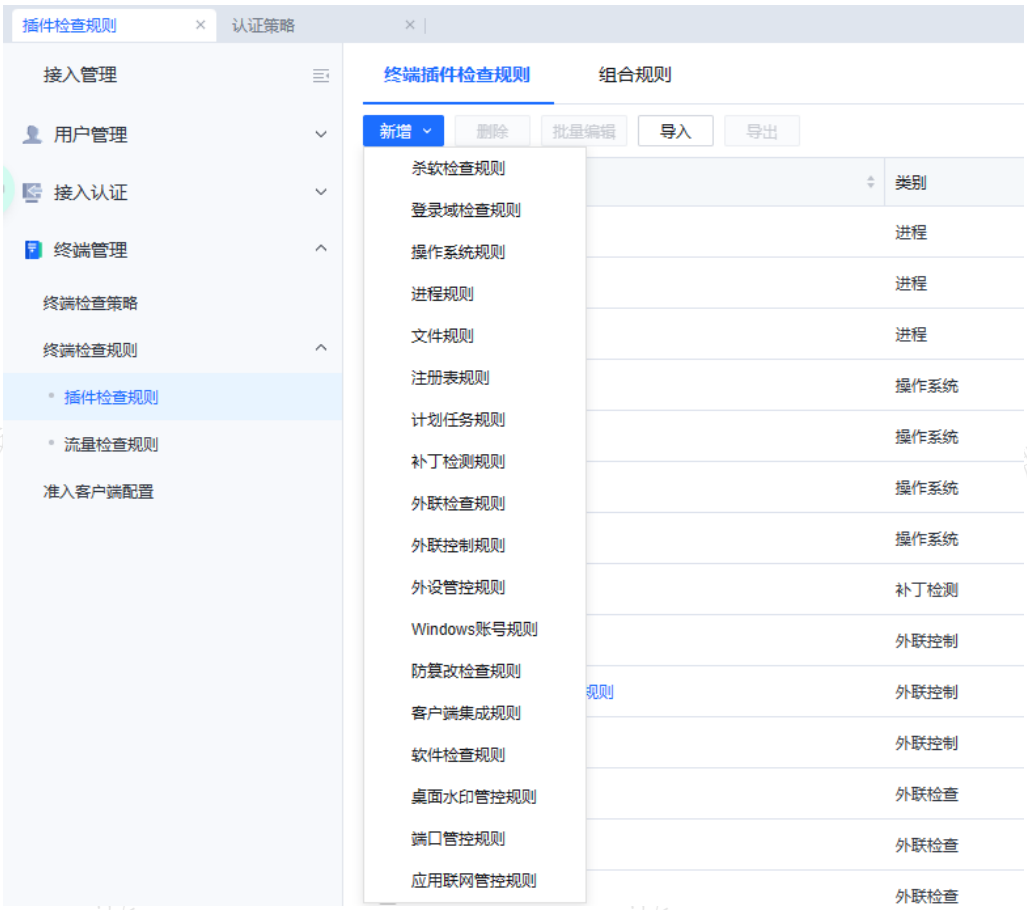
路径：知识库/资料库。

操作系统场景介绍

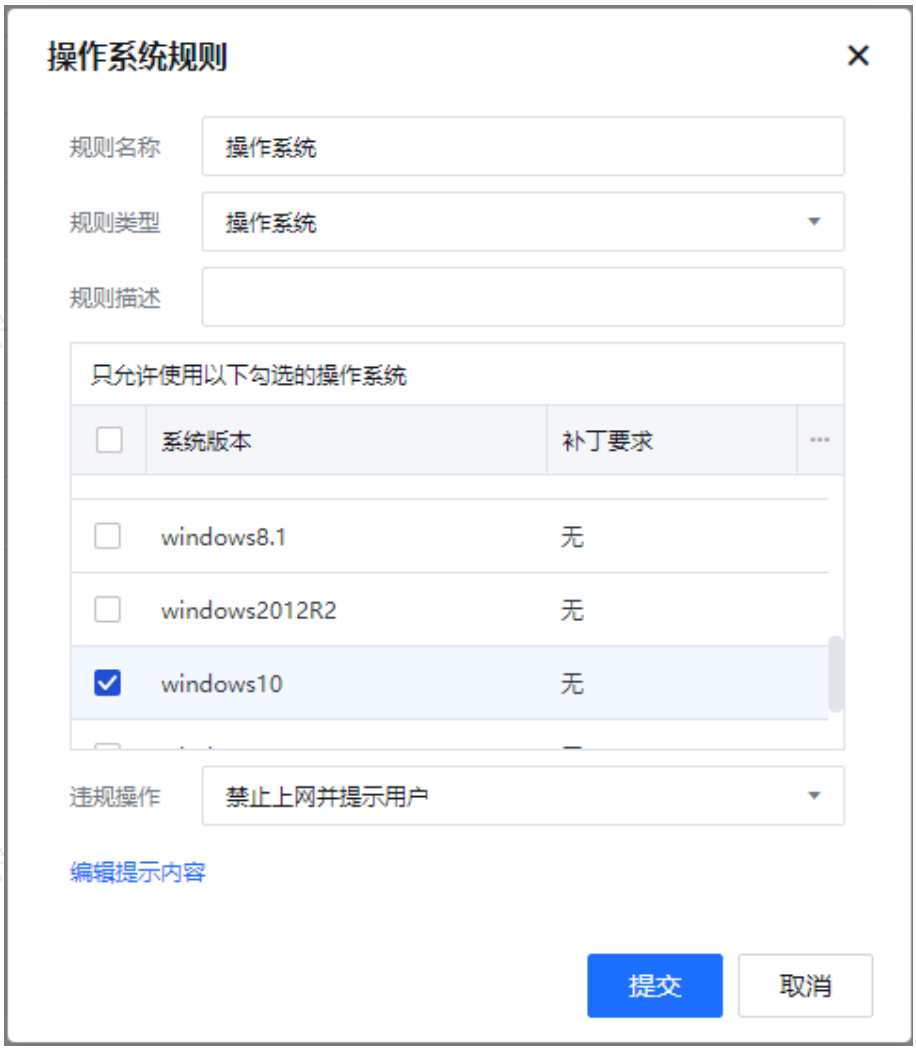
当某企业只允许员工使用windows10的操作系统时，对接入终端的操作系统进行合规性检查，使用合规的操作系统能正常上网。对于不合规的终端有三种处理方法：可禁止上网并提示用户、只提示用户、只记录结果。

操作步骤

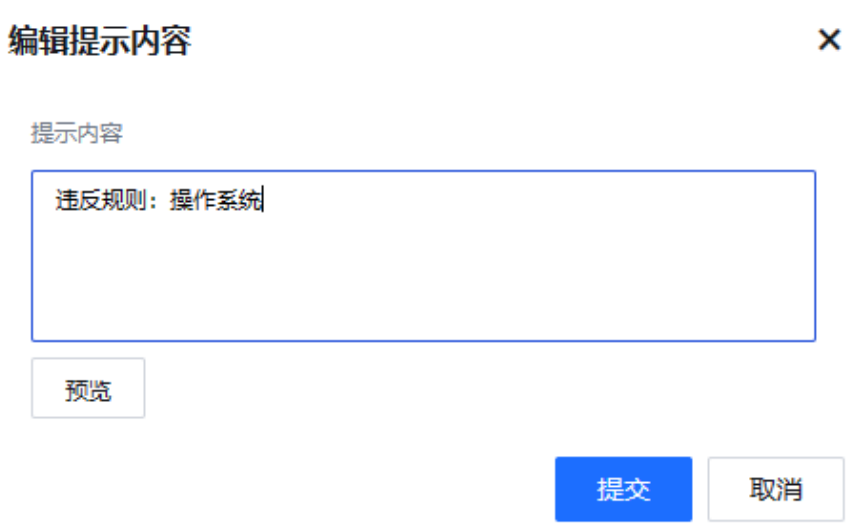
步骤1.在[接入管理/终端管理/终端检查规则/终端插件检查规则]，点击<新增>一条[操作系统规则]。



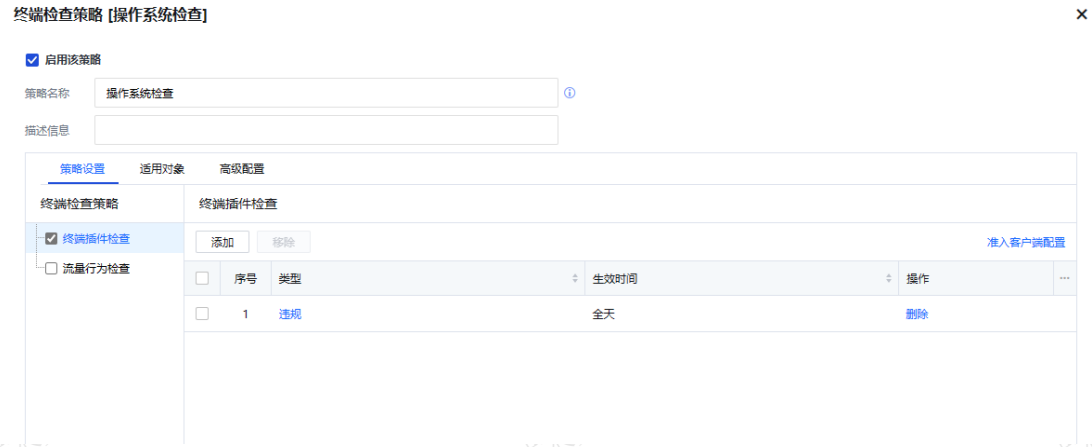
步骤2.在操作系统规则的页面中填入规则名称、规则类型、规则描述，勾选相应的操作系统，这里勾选的操作系统是未违规的，未勾选的操作系统都是违规的，这里以windows10系统为例，只允许使用windows10系统，其他未勾选系统均为违规系统。



步骤3.针对违规操作有的方式有：禁止上网并提示用户、只提示用户、只记录结果，同时点击[编辑提示内容]可自定义提示内容。



步骤4.完成检查规则设置之后，在导航菜单中的[接入管理/终端检查/检查策略]里新建一条策略，输入策略名称和描述信息，勾选终端插件检查，点击<添加>。选择之前创建的操作系统规则，生效时间按需选择，然后点击<确定>。

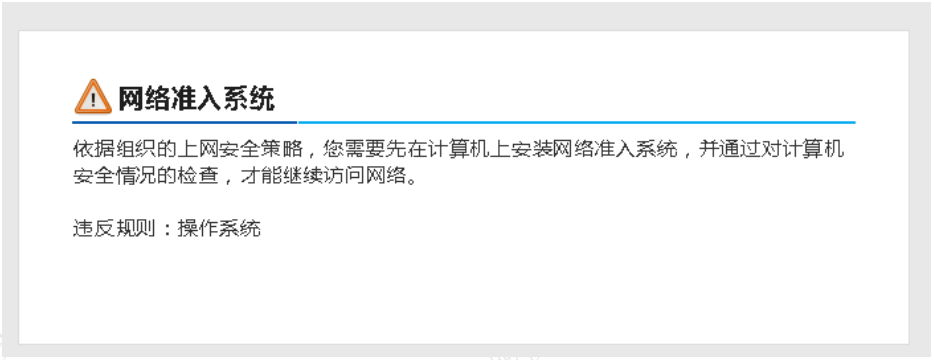


步骤5.在[适用对象]页面选择该策略生效的用户，可以根据用户、位置、终端类型、目标区域选择。

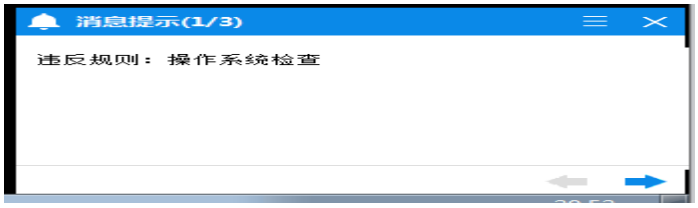
步骤6.在[高级配置]页面可设置该策略过期时间、同级别管理员查看编辑权限设置、是否允许低级别管理员查看。

步骤7.点击<提交>，至此完成操作系统检测功能配置，且在检查策略列表看到刚才配置的操作系统检查策略。

步骤8.当用户在没有使用规定的操作系统，访问互联网会出现禁止上网。



步骤9.设备会弹出提示违反规则提示：操作系统检查。



行为管理

网络应用极其丰富，随着大量社交型网络应用的出现，用户将个人网络行为带入办公场所，由此引发各种管

理和安全问题。行为管理模块可对不同用户上网的行为进行管控，可进行精细化管控，帮助管理员透彻了解网络应用现状和用户行为。

行为管理通过设置上网权限策略，可分别根据用户类型、位置、终端类型和目标区域设置不同的策略。

上网代理

AC设备通过上网代理功能可作为内网终端设备的代理服务器，终端用户可通过AC设备代理上网，管理员可通过AC设备管理终端用户的上网行为。

说明

“上网代理”相关功能模块的配置界面在设备未激活“上网代理授权”时处于隐藏状态。

代理服务

在代理服务栏用于配置代理的方式类型，目前支持的方式有HTTP代理、SOCKS4/SOCKS5代理以及PAC代理（自动配置脚本代理）。

启用HTTP代理：用于配置HTTP代理相关信息，代理端口最多支持5个，多个端口以逗号隔开。点击HTTP代理下的<高级选项>，可配置保留客户端源IP信息。

两种保留方式的应用场景如下所示:

• X-Forwarded-For：我们熟知的代理上网场景是为了隐藏源IP，但是有些时候通过CDN后到达nginx做负载均衡时需要请求头中的X-Forwarded-For字段，而字段内容是发起HTTP请求的客户端的真实IP。

• X-Forwarded-By：做反向代理的设备用于添加的到后端代理服务器的信息场景。

启用SOCKS4/SOCKS5代理：用于开启SOCKS4/SOCKS5代理，并设置代理的端口号；最多支持填写5个端口，多个端口时以逗号分隔。

启用自动配置（PAC）脚本：通过统一的PAC脚本配置，当浏览器访问网页的时候会根据脚本文件里面界定的内容来访问。一个基本用法是用来实现在终端选择哪部分域名走代理，哪部分域名走系统路由。

脚本地址为：http://代理上网的IP地址/proxy.pac，如：http://10.111.111.8/proxy.pac。点击编辑脚本，界面如下：

□导入脚本：支持直接导入PAC文件；

□下载示例模板：提供脚本使用帮助和示例模板；

□恢复到默认：支持恢复到默认配置；

□可直接编辑修改，提交后生效

代理策略

[代理策略]可以分别对HTTP代理、SOCKS4代理、SOCKS5代理配置策略，以满足客户多样性的需求。代理策略工具栏支持新增，删除，启用，禁用，上移，下移功能。

HTTP代理策略

HTTP代理策略配置介绍，点击[新增/HTTP代理策略]，界面如下：

• 启用：用来控制代理策略的开启或禁用。

• 名称：填写HTTP代理策略的名称。

• 描述：添加代理策略的描述信息。

• 适用对象：配置代理策略的源对象，支持源IP、本地认证用户、域用户、终端类型，默认所有适用对象。

• 目的域名：可以自定义选择AC设备内置域名分类，或手动指定域名地址，默认选择所有域名（指定的域名：支持标准的域名，如果填入baidu.com，那么对zhidao.baidu.com，music.baidu.com都生效，如果填入www.baidu.com表示只对这一个域名生效。单个域名长度最大支持127个字节，最大容量支持1000个）。

• 动作：可以选择允许或者拒绝，默认值是允许。

• 请求ICAP服务器组：用于配置将用户发起的请求数据发送到请求ICAP服务器组，默认选择“无”，不使用请求服务器ICAP服务器。

• 响应ICAP服务器组：用于配置将服务器的响应数据发送到响应ICAP服务器组，默认选择“无”，不使用响应服务器ICAP服务器。

• 二级代理：用于配置数据是否要进行二级代理。可以选择一个二级代理服务器或者新增一个。默认选择“无”。二级代理服务器的配置见5.4节的介绍。

• 代理上网IP：选择使用设备的某个IP地址代理上网。有两种选择方式：一种是绑定设备的某个接口IP地址，如果选择绑定展开后系统将设备所有接口可用IP地址列出来给用户选择，会列出WAN、BR、DMZ口、VLAN地址、单臂口的所有IP，会自动排除链路地址和LAN口地址。另一种自动选择出口IP。

请求/响应ICAP服务器组检查方式

ICAP功能模块支持请求、响应方向的检查，每个方向能同时支持使用两台ICAP服务器检查，当HTTP代理策略中存在两台“请求/响应ICAP服务器组”时，可以通过轮询、并发AND和并发OR三种检查方式。

• 轮询：按照列表顺序依次将数据转发到ICAP服务器组，当第一台ICAP服务器组检查结果为拒绝时，请求将会终止转发，不会继续转发给后续的ICAP服务器组，直接返回拒绝结果；ICAP服务器检查结果均为通过时，检查结果才为通过。

• 并发AND：将数据同时发往列表中的ICAP服务器组，并同时接收返回的结果，只要收到一台ICAP服务器的返回拒绝则认为检查结果为不通过；所有ICAP服务器均返回OK时，结果才为通过。

• 并发OR：将数据同时发往列表中的ICAP服务器组，并同时接收返回结果，只要收到一台ICAP服务器返回OK，则认为检查结果为通过。

• 最长等待时间：设置检查时最长等待时间，超过等待时间则会进行失败或放通处理。默认为检查失败。

• 超时动作：“视为检查失败”将超时后的检查结果视为失败；“视为检查通过”将超时后的检查结果视为通过。

• 供应商拒绝页面：启用供应商拒绝页面时，ICAP服务器将拒绝页面重定向到终端PC，否则默认重定向到AC拒绝页面。

• 邮件告警：当ICAP检查结果为失败或发生超时，将发送邮件告警，需要配置邮件通知服务器。

⚠ 注意

1.一条代理策略最多只能同时添加两个请求服务器和两个响应服务器。

2.开启数据直通代理流量不会发送到ICAP服务器。

SOCKS4代理策略

在代理策略配置页面点击[新增/SOCKS4代理策略]，即可配置SOCKS4代理策略。

- 启用：用来控制代理策略的开启或禁用
- 名称：填写SOCKS4代理策略的名称
- 描述：添加代理策略的描述信息
- 源IP组：选择策略适用的源IP地址，以IP组为单位。可以直接引用[对象定义]中的IP组。可以选多个源IP组，默认选择全部。
- 目的域名：可以自定义选择AC设备内置域名分类，或手动指定域名地址，默认选择所有域名（指定的域名：支持标准的域名，如果填入baidu.com，那么对zhidao.baidu.com，music.baidu.com都生效，如果填入www.baidu.com表示只对这一个域名生效。单个域名长度最大支持127个字节，最大容量支持1000个）。

• 动作：可以选择允许或者拒绝。默认是允许。

• 二级代理：用于配置数据是否要进行二级代理。可以选择一个二级代理服务器或者新增一个。默认选择“无”。二级代理服务器的配置见5.4节的介绍。

• 代理上网IP：选择使用设备的某个IP地址代理上网。有两种选择方式：一种是绑定设备的某个接口IP地址，如果选择绑定展开后系统将设备所有接口可用IP地址列出来给用户选择，会列出WAN、BR、DMZ口、VLAN地址、单臂口的所有IP，会自动排除链路地址和LAN口地址。另一种自动选择出口IP。

SOCKS5代理策略

在代理策略配置页面点击[新增/SOCKS4代理策略]，即可配置SOCKS5代理策略：

• 启用：用来控制代理策略的开启或禁用

• 名称：填写SOCKS5代理策略的名称

• 描述：添加代理策略的描述信息

• 源IP组：选择适用的源IP地址，以IP组为单位。直接引用系统对象定义中的IP组，可以选多个。默认为全部。

• 目的域名：可以自定义选择AC设备内置域名分类，或手动指定域名地址，默认选择所有域名（指定的域名：支持标准的域名，如果填入baidu.com，那么对zhidao.baidu.com，music.baidu.com都生效，如果填入www.baidu.com表示只对这一个域名生效。单个域名长度最大支持127个字节，最大容量支持1000个）。

• 动作：可以选择允许或者拒绝，默认是允许。

• 二级代理：用于配置数据是否要进行二级代理。可以选择一个二级代理服务器或者新增一个。默认选择“无”。二级代理服务器的配置见5.4节的介绍。

• 代理上网IP：即设备用哪个IP地址代理上网。有两种选择方式，一种是绑定设备的某个IP地址，系统自动将设备的IP地址列出来给用户选择，会列出WAN、BR、DMZ口、VLAN地址、单臂口的所有IP，排除链路地址和LAN口地址。另一种自动选择出口IP。

说明

1.当所有的代理服务（HTTP代理，SOCKS4代理，SOCKS5代理）都没有启用时，在代理 策略页面用红色字体提示：当前代理服务没有开启，代理策略不会生效。

2.代理策略从上到下依次匹配，一个连接仅能匹配到一条策略。

3.代理策略最多支持512条。

4.代理没有默认策略，默认的行为都是允许。即只要开启了代理服务（HTTP,SOCKS4，SOCKS5），那么对应的代理数据默认就会放通。

ICAP服务器组

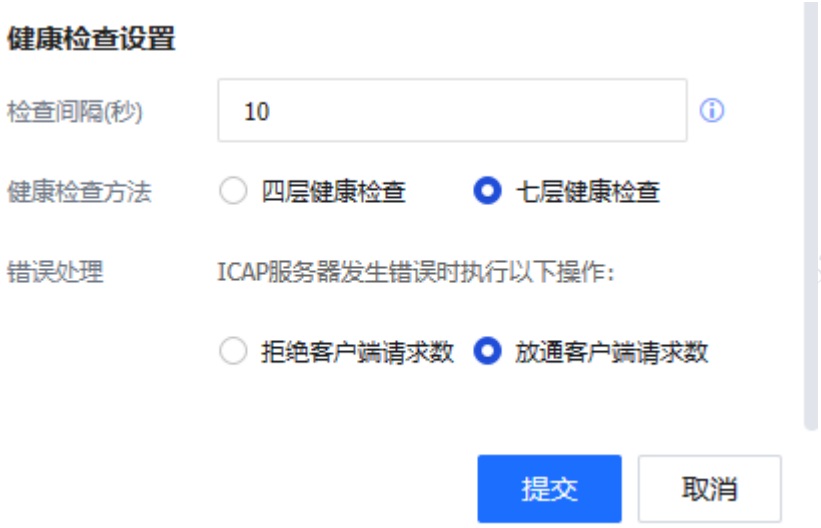
ICAP，即 Internet Content Adaptation Protocol，本质上是在HTTP message上执行RPC远程过程调用的一种轻量级的协议。通过ICAP可以将HTTP message发送到ICAP服务器进行内容检查，当前AC设备ICAP功能模块支持http(s)的请求和响应两个方向的安全检查，可以全方位的覆盖所有http(s)流量，避免出现数据泄密、下载病毒等风险。

[ICAP服务器组]用于配置ICAP服务器，用户数据经过设备代理之后，可发送到ICAP服务器实现代理后杀毒、DLP等操作。

支持配置的ICAP服务器组数量上限为64个，一个ICAP组可以包含一个或者多个ICAP服务器,一个ICAP服务器组最多支持添加32个ICAP服务器，ICAP组内可以实现轮转负载（将请求按照顺序分发的方式分发送到组内一个ICAP服务器上）。ICAP组之间不允许包含相同的服务器，即一个ICAP服务器只能属于一个组。ICAP服务器地址和端口可以作为唯一标示来标识一个服务器。

新增ICAP服务器组

在ICAP服务器配置页面，点击<新增>按钮即可配置ICAP服务器相关信息。



□名称：填写服务器组名称

□描述：可添加ICAP服务器组的描述信息，便于区分管理。

检查类型

根据检查类型不同，AC设备支持添加请求检查ICAP服务器和响应检查ICAP服务器。

• 请求检查ICAP服务器组

□请求类型：包含POST、GET和PUT三种ICAP请求类型。

□最小转发阈值：请求数据超过或等于该值时才转发到ICAP服务器，默认1KB。

□最大连接数：支持配置请求方向的同时最大处理连接会话数。超过或等于此大小时，会话将被置于积压状态，建议采用默认值或最佳配置（在新增ICAP服务器时，点击协商按钮，AC会与ICAP服务器进行最大连接数协商，获取最佳配置）。

□连接积压：支持配置单个连接最大等待处理连接会话数。例如连接积压为10，则当某个连接的当前请求尚未完成时，新的请求会被置于等待状态，当已处于等待状态的请求数超过10个时，新增的请求将会被直接放通。默认连接积压数为10。

□请求改写：启用此功能后，将会在转发给ICAP服务器的URL后拼接增加已选中的字段，拼接后，原始请求URL将会发生变化。拼接顺序为：显示名、用户名、部门信息、自定义内容。

• 响应检查ICAP服务器组

□最小转发阈值：响应数据超过或等于该值时才转发到ICAP服务器，默认10KB。

□检查内容白名单：配置检查内容白名单，当响应数据携带已勾选白名单内容时，将不做ICAP检查。

□支持配置响应方向的同时最大处理连接会话数。超过或等于此大小时，会话将被置于积压状态，建议采用默认值或最佳配置（在新增ICAP服务器时，点击协商按钮，AC会与ICAP服务器进行最大连接数协商，获取最佳配置）。

□连接积压：支持配置单个连接最大等待处理连接会话数。例如连接积压为10，则当某个连接的当前请求尚未完成时，新的请求会被置于等待状态，当已处于等待状态的请求数超过10个时，新增的请求将会被直接放通。默认连接积压数为10

□请求改写：启用此功能后，将会在转发给ICAP服务器的响应URL后拼接增加已选中的字段，拼接后，原始URL将会发生变化。拼接顺序为：显示名、用户名、部门信息、自定义内容。

服务器配置

在新增服务器组配置页面点击<新增服务器>，即可进入添加ICAP服务器的配置页面。

□名称：填写ICAP服务器名称。

□描述：填写ICAP服务器描述信息。

□ICAP地址：配置ICAP地址（支持IPV6），最多支持96个字符串。

□ICAP端口：配置ICAP端口，ICAP端口合法范围为1-65535。

□连接超时时间：超时时间单位为s，范围为1-120。

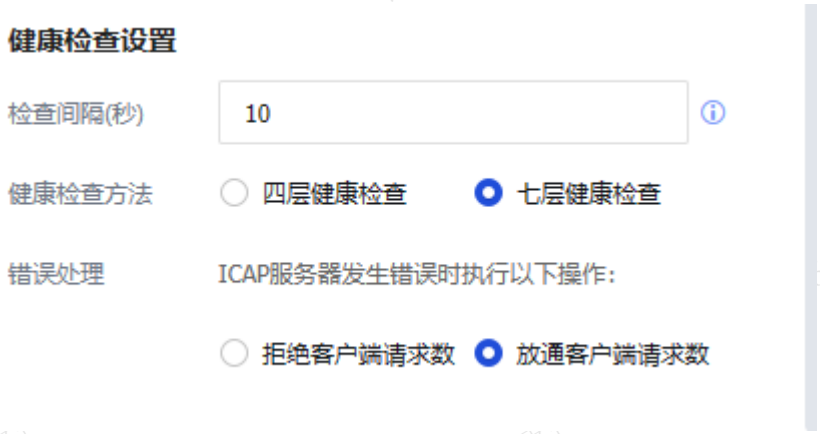
□最大连接数：最大连接数范围为4-100。

□附加发送内容：可以选择附加发送给内容，可附加的信息有源IP地址、目的IP或域名、经过认证的用户、经过认证的用户组。

□协商：用于测试设备与ICAP服务器之间的连通性，支持与ICAP服务器进行参数协商。

健康检查设置

在健康检查设置栏可以配置健康检查机制，支持配置的检查间隔时间为5-60s，默认为10s。可配置四层健康检查和七层健康检查；四层通过TCP探测服务端口，七层通过ICAP协议探测ICAP服务器是否可达。当ICAP服务器发生错误时，可以选择拒绝客户端请求或者放通客户端请求。



说明

当ICAP服务器发生错误时：

1.拒绝客户端请求数据：丢弃终端代理数据，终端将无法通过AC设备代理转发。

2.放通客户端请求数据：跳过ICAP服务器，直接转发代理数据。

ICAP服务器组状态

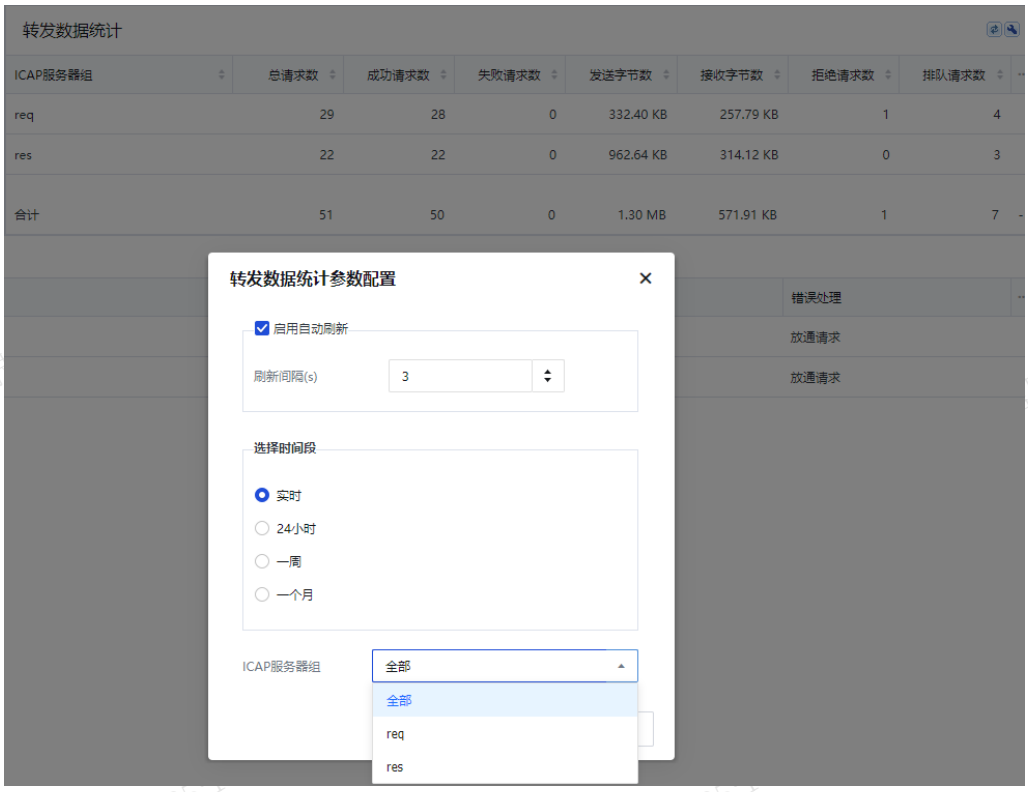
完成ICAP服务器配置后，将会展示ICAP服务器转发的流量信息状态（包含请求数、成功/失败请求数、发送字节数等信息）。

ICAP服务器组状态可视化前置条件：

1. 启用HTTP代理。
2. 需要在代理策略中新增HTTP代理策略并配置请求ICAP服务器组或响应ICAP服务器组。命中代理策略的http(s)数据才会进行请求或响应ICAP服务器检查。
3. 配置ICAP服务器组后才会生成对应的展示数据。
4. 删除ICAP服务器组后删除展示数据。

ICAP服务器组转发数据监测折线图可设置刷新间隔、数据显示时间段、及指定ICAP服务器组。

ICAP服务器组转发数据统计状态可设置刷新间隔、数据显示时间段、及指定ICAP服务器组。



说明

1. 可在[系统管理/系统配置/告警选项/告警事件]启用ICAP检查告警，当ICAP检查失败时，会产生邮件告警。

2. 可在内置/外置日志分析平台的[日志中心/上网安全]查看ICAP检查失败时产生的安全日志。

二级代理服务器

当设备需要通过其他的代理服务器才能访问业务的环境下，则需要为设备配置“二级代理服务器”。在[上网代理/二级代理服务器]页面点击<新增>按钮进入二级代理服务器配置页面。

填写二级代理服务器的名称、描述、IP地址和端口后。点击<测试有效性>，测试设备与代理服务器之间的连通性。

若二级代理服务器需要对设备进行身份验证，则需要填写相应的用户名、密码。

Forward配置

当企业用户将业务服务器发布到公网后，员工为了更加方便的访问业务服务器往往会直接访问该业务服务器的公网IP或者域名。如果此时员工在内网访问该业务服务器的公网IP或者域名，那么流量需要先到公网然后从公网转发回内网服务器，此时无疑会增加出口设备的负载压力，通过AC代理模块的Forward转发功能即可将此场景下的流量直接发送到内网服务器，流量不再需要先转发到公网再绕回内网，从而减轻出口设备压力。

Forward功能针对http、https、socks三类代理数据，将发往特定目标地址和端口的数据转到指定的IP和端口，以实现数据转发的目的。[目的地址]和[目的端口]用于标识需要转发的流量，其中[目的地址]可以配置域名或者IP。而[Forward IP]和[Forward]端口用于标识接收转发后的流量的服务器。

支持配置[域名/IP+端口]Forward转发到[IP+端口]。如果[目的地址]栏配置为域名，而代理的流量目的地址

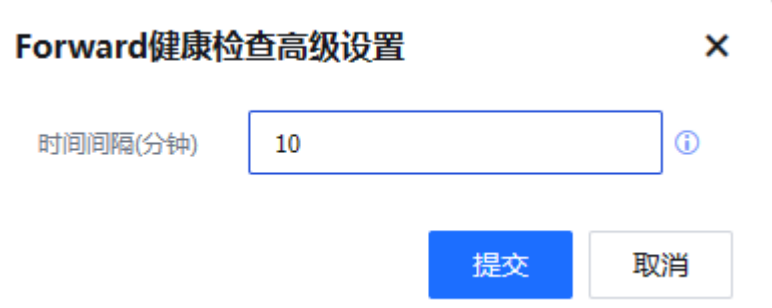
为此域名解析后的IP，那么将不会匹配到Forward规则。

例如：规则配置里目的地址配置为www.sangfor.com，该域名解析后的IP为3.3.3.3。只有代理的流量的目的地址为www.sangfor.com时才会匹配转发规则。如果代理的流量的目的地址为3.3.3.3则不会匹配到此规则。

□健康检查设置：对forwarding服务器的连通性做健康检查，即探测连通性是否正常。探测方式可以选择用四层健康检查还是七层健康检查，七层健康检查时要发（HTTP和HTTPS探测包）；

□异常处理方法：用于选择通过健康检查配置探测到forwarding服务器故障时的处理动作。

□高级设置：配置健康检查的时间，时间间隔全局生效，即存在多个Forward规则时，该配置会应用到全部的Forward规则。时间范围可为5~60分钟



访问权限策略

访问权限策略模块对用户上网进行管理，管理员可以根据内网用户的权限分配情况，设置不同的访问权限策略。访问权限策略包括访问权限策略和SSL解密策略。

访问权限策略包括应用控制、SaaS管理、邮件过滤和QQ号白名单。应用控制包括[应用控制]、[端口控制]、[代理控制]、[Web关键字过滤]、[Web文件类型过滤]、[SaaS高级选项]。

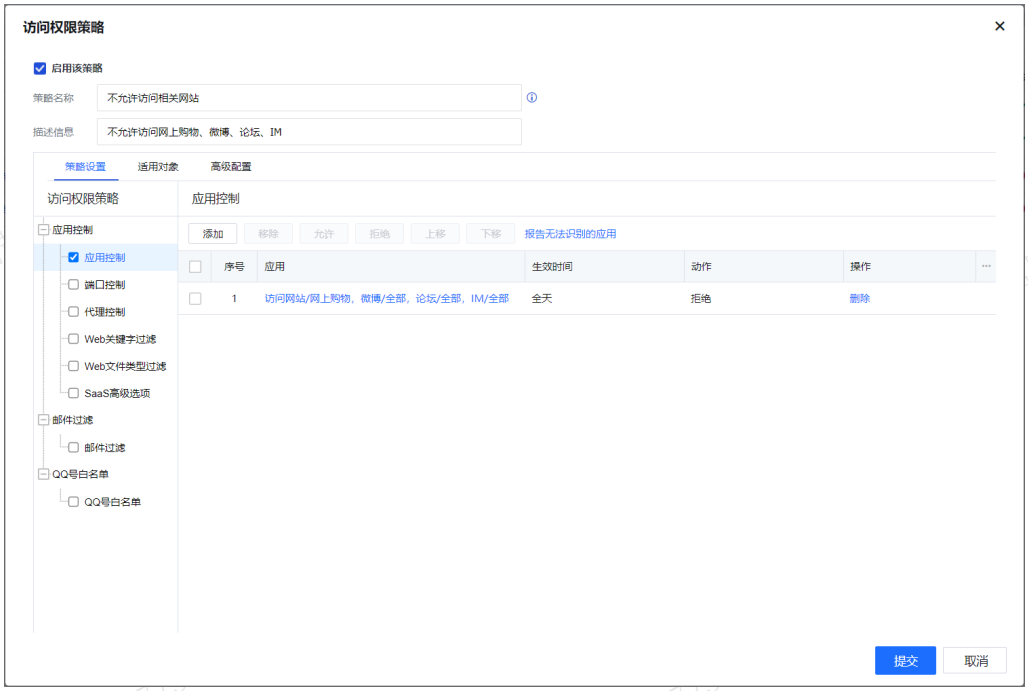
表15访问权限功能说明

操作	功能说明
应用控制	设备中有针对各种常见网络应用设置的应用规则库和针对访问网站的URL分类库的规则，实现对网络应用的权限控制和对访问各类网站的权限控制。
端口控制	是通过对数据包的IP地址、协议号、端口号进行检测，从而实现对上网数据的控制，可以在[系统管理/对象定义/ IP组]中设置需要控制目标IP组，在[对象定义/网络服务]中设置需要控制的目标协议或端口，端口控制正是引用这些对象，实现的上网数据控制。
代理控制	包括是否允许HTTP代理、SOCK代理的选项，是否使用防共享上网检测等。可以通过这些选项，来设置内网用户是否可以使用HTTP代理、SOCK代理和防共享上网检测等。选项[不允许在HTTP，SSL协议的标准端口上使用其它协议]用于防止一些应用程序使用标准的HTTP端口（TCP 80）和SSL端口（TCP 443）来传输自己的数据，从而逃避设备的限制。
Web关键字过滤	包括[搜索引擎搜索词]和[HTTP上传]，其中前者是对在搜索引擎上搜索的关键字进行过滤或告警，后者是对通过HTTP协议上传的关键字进行过滤或告警，引用的关键字是[系统管理/对象定义/关键字组]中定义的关键字。 注意：两者的设置都是针对所有HTTP网站的，这里无法对指定的URL进行关键字的过滤或告警。
Web文件类型过滤	可以设置通过HTTP协议和FTP协议上传和下载的文件类型过滤。 引用的文件类型是[系统管理/对象定义/文件类型组]中定义的文件类型。
SaaS高级选	SaaS高级选项配置包括Google、Youtube、Office365、Bing Search、Facebook、Dropbox等设置。上述功能需要开启SSL解密策略才能支持。

项	
QQ号白名单	对指定的QQ号进行放通，封堵其它QQ号码；支持PC和移动QQ应用。
邮件过滤	用于对内网客户端通过SMTP协议发送的邮件进行过滤，过滤的条件可以设置收发邮件地址，邮件标题和正文的关键字等。

新增访问权限策略

步骤1.在[行为管理/访问权限策略]，点击<新增>选择[访问权限策略]，进入新策略编辑界面，勾选<启用该策略>，策略才会生效。



步骤2.填写策略名称和描述信息，其中策略名称为策略的唯一标识，不能重复，为必填项。描述信息是策略的概要，非必填项。

步骤3.点击<策略设置>，根据需要设置相应的上网权限策略，在访问权限策略设置控制类型，访问权限策可选项包括：应用控制、SSL管理、邮件过滤、QQ白名单。可参考访问权限策略分类配置指导。

步骤4.点击<适用对象>，此处选中的用户/位置/终端类型/目标区域将全部匹配此上网策略设置的权限。

步骤5.点击<高级配置>，设置包括策略过期日期设置、同级别管理员查看编辑权限设置、允许低级别管理员查看。

其中：

• 策略过期日期设置：是设置该策略的生效期。如果设置为[永不过期]，则策略将永久有效。如果设置[过期时期]，比如选择日期为2015-06-01，则表示此策略在2015-06-01之后过期，成为无效策略。

• 同级别管理员查看编辑权限设置：有两种权限可以选择[允许查看]和[允许编辑]。此处的“同级别管理员”指的是在[系统管理/系统配置/管理员账户]中属于同一角色的管理员，如果勾选[允许查看]，则同级别管理员可以查看此策略，而不能进行修改。如果勾选[允许编辑]，则同级别管理员默认拥有[允许查看]权限，并且可以对此策略进行修改。

• 允许低级管理员查看：勾选此项，则低级管理员可查看此策略，权限只限于查看，不能修改策略。“低级管理员”指的是在[系统管理/系统配置/管理员账户]中设置的角色级别低于建立此策略的管理员级别的管理员。

步骤6.设置完成，点击<提交>，完成访问权限策略配置。

步骤7.当适用范围的用户去访问网上购物网站时会被拒绝。

访问权限策略分类

访问权限策略配置的类型有应用控制、端口控制、代理控制、Web关键字过滤、Web文件类型过滤、SaaS高级选项、邮件过滤、QQ号白名单等策略的配置，管理员配置过程可参考新增访问权限策略配置。

应用控制

应用控制策略是通过针对各种常见的网络应用设置的应用规则库和网站的URL分类库，实现网络应用的控制和对访问各类网站的控制。

应用控制的检测方式有两种：

• 对数据包的内容进行检测，从而实现控制某些应用的目的。针对各种已经识别或者未被识别应用服务控制，如对淘宝网站、P2P应用、QQ、邮件等，设置相对应的控制策略。

• 对访问网站的行为进行过滤，包括HTTP URL过滤、HTTPS URL网站过滤及HTTP上传过滤。

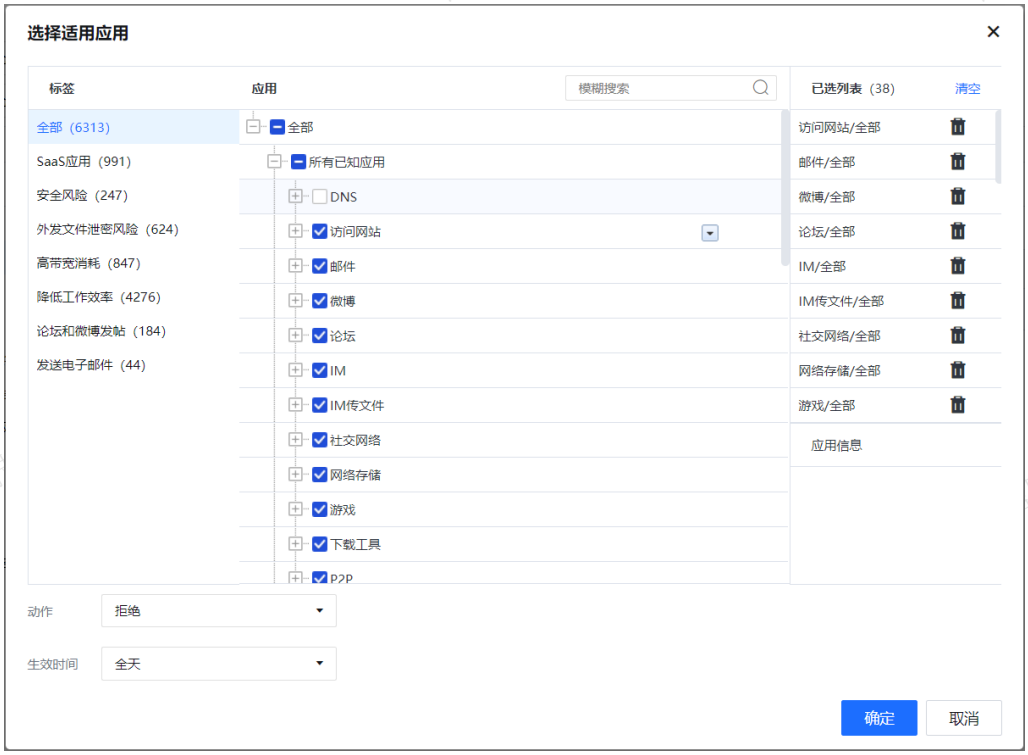
接下来介绍以下两种场景配置指导：应用类型控制和网站指定URL进行控制。详细配置可参考新增访问权限策略章节。

针对应用类型进行控制

步骤1.在[行为管理/访问权限策略]，点击<新增>，选择[访问权限策略]，进入新策略编辑界面，勾选<启用该策略>，策略才会生效。

步骤2.填写策略名称和描述信息，其中策略名称为策略的唯一标识，不能重复，为必填项。描述信息是策略的概要，非必填项。

步骤3.点击<策略设置>，勾选应用控制，进入应用控制编辑页面，点击<添加>按钮并弹出选择适用的应用框页面。



步骤4.勾选需要控制的应用，动作可选允许或拒绝，生效时间，默认是全天，也可自定义设置，点击<确定>完成应用类型配置。生效时间的具体设置参考时间计划组设置。

步骤5.如果需要修改已设置的应用控制策略。勾选需要修改的应用，可以点击<移除>来删除掉该策略。点击<允许>可以把策略动作改为允许。点击<拒绝>则把策略动作改为拒绝。点击<上移>和<下移>，则可以把策略的序号进行调整。在进行策略规则匹配的时候，序号靠前的策略优先被匹配到。

步骤6.如果此策略中您只需要做应用控制，则点击<提交>按钮完成此策略的编辑，如果您还需要编辑其他类型的策略，则继续选择其他控制类型进行编辑。

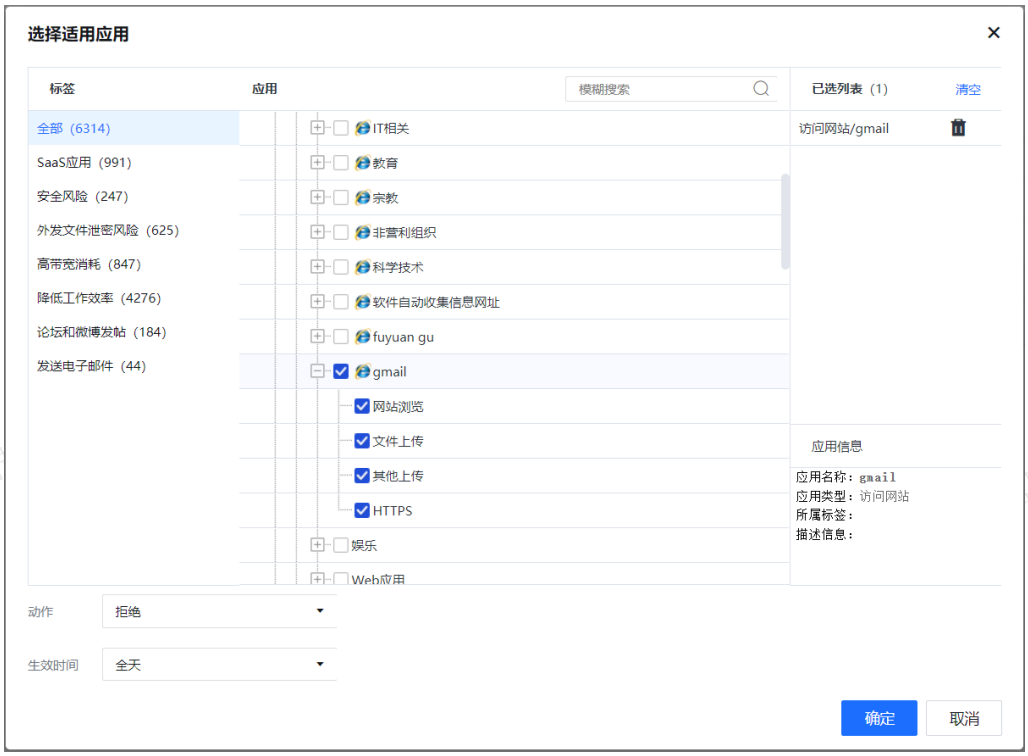
针对指定的URL进行控制

HTTPS URL过滤是对使用HTTPS协议访问的网站进行过滤。例如拒绝内网用户访问加密网站https://mail.google.com/。

步骤1.因为URL分类库中默认没有一个URL组是专门对应https://mail.google.com/的，所以在设置规则之前，需要先建一个URL组，将https://mail.google.com/添加进去。

步骤2.进入[系统管理/对象定义/URL分类库]页面，点击<新增>按钮，进入URL组设置页面，输入URL组名称、URL组描述以及URL。由于HTTPS URL也支持通配符，所以URL设置成：*.google.com。

步骤3.在[行为管理/访问权限策略]，新增一条访问权限策略，点击<策略设置>，勾选应用控制，进入应用控制编辑页面。



步骤4.点击<添加>按钮，弹出选择适用应用框。找到“访问网站”这一类别，找到上一步中自定义的URL组“gmail”。动作可选允许或拒绝，生效时间，默认是全天，也可自定义设置，点击<确定>完成应用类型配置。生效时间的具体设置参考时间计划组设置。

说明：

从AC12.0.42版本起，设备识别https的网站会先查client hello中的server name字段，如果没有这个字段，不再通过证书重组来获取证书中的“颁发给”作为识别依据。而是通过DNS cache功能，即终端的域名访问流量经过AC时，AC通过DNS cashe里的IP和域名的对应表来识别终端访问的域名。

端口控制

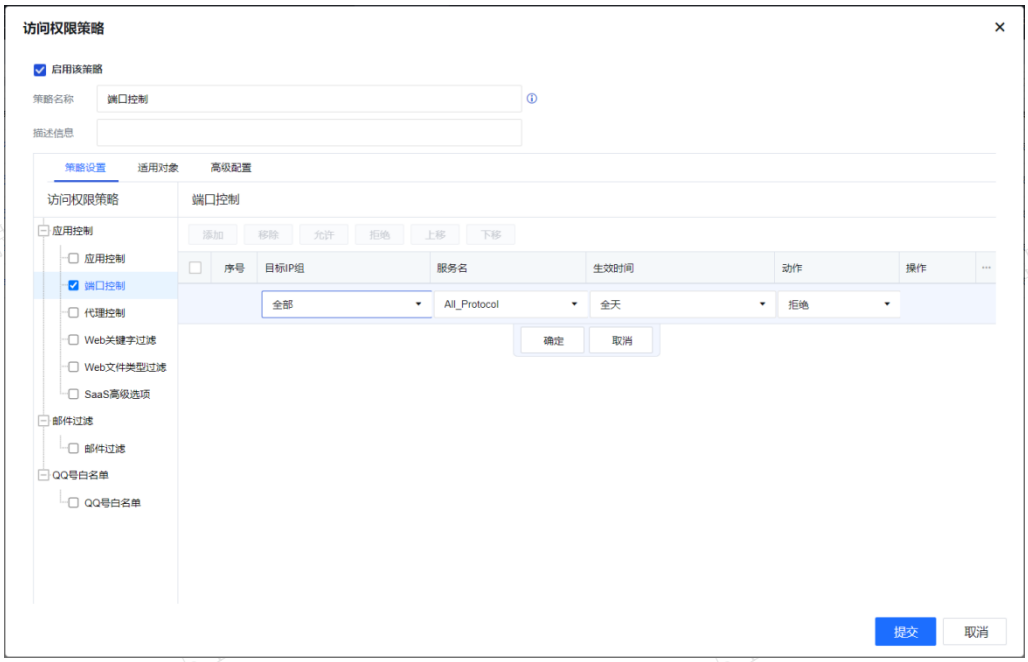
端口控制是针对数据包的目标IP、端口、时间段等进行控制的一种方法。当管理员需要对某个IP或者IP组的端口进行策略控制时，可配置端口控制进行实现。设备对其他未设置的网络服务默认是允许访问的。

操作步骤

步骤1.在[行为管理/访问权限策略]，点击<新增>，选择[访问权限策略]，进入新策略编辑界面，勾选<启用该策略>，策略才会生效。

步骤2.填写策略名称和描述信息，其中策略名称为策略的唯一标识，不能重复，为必填项。描述信息是策略的概要，非必填项。

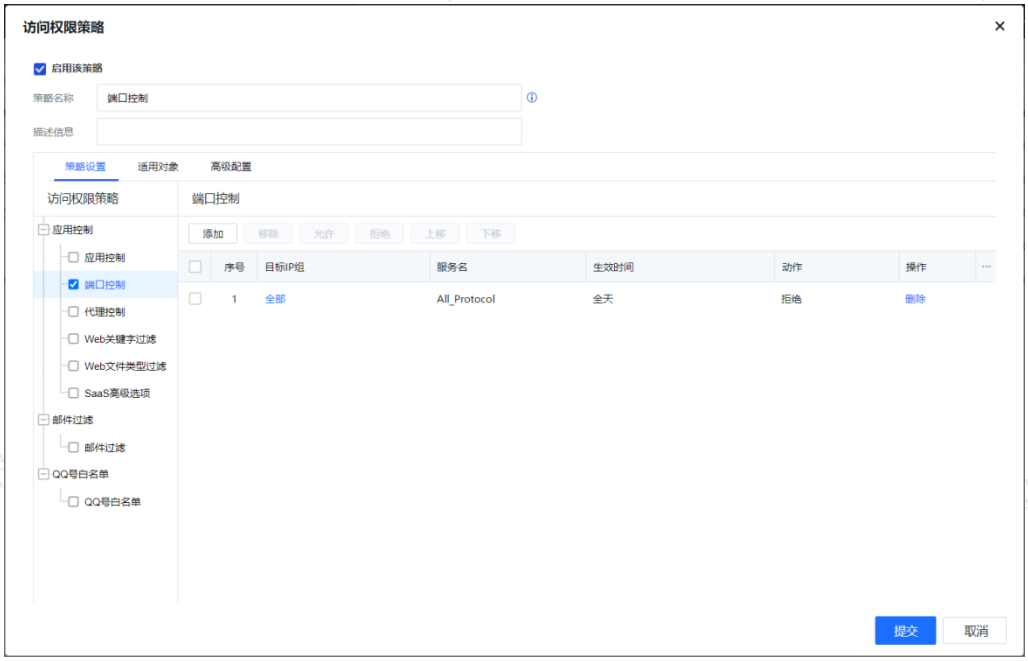
步骤3.点击<策略设置>，勾选端口控制，进入端口控制编辑页面，点击<添加>按钮，添加规则。



步骤4.添加目标IP组，点击下拉框，在下拉列表中选择对应的IP组。如果不存在需要的IP组，可以点击下拉框最下方的[新增IP组]选项进行添加。设置好相关IP组信息后，点击<提交>，完成IP组设置。

步骤5.添加服务名，点击下拉框，在下拉列表中可以选择的服务有：All_Protocol、DNS、HTTPS、SMTP、POP3、LDAP、FTP等。如果不存在需要的服务，可以点击下拉框最下方的[新增网络服务]选项进行添加。设置好相关网络服务信息后，点击<提交>，完成网络服务设置。

步骤6.返回到之前的配置界面，设置动作为拒绝，动作生效时间为上班时间，点击<确定>。完成此策略的设置。

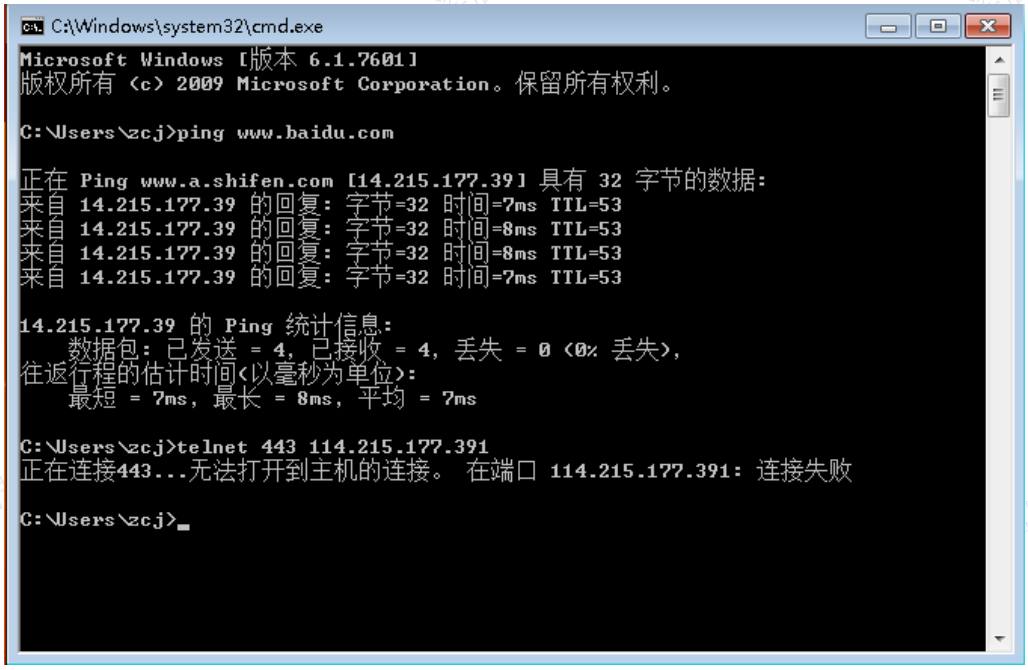


步骤7.如果需要修改已设置的端口控制策略。勾选需要修改的网络服务，可以点击<移除>来删除掉该策略。点击<允许>可以把策略动作改为允许。点击<拒绝>则把策略动作改为拒绝。点击<上移>和<下移>，则可以把策略的序号进行调整。在进行策略规则匹配的时候，序号靠前的策略会先被匹配到。

步骤8.如果此策略中只需要做端口控制，则点击<提交>按钮完成此策略的编辑，如果还需要编辑其他类型的策略，则继续选择其他控制类型进行编辑。

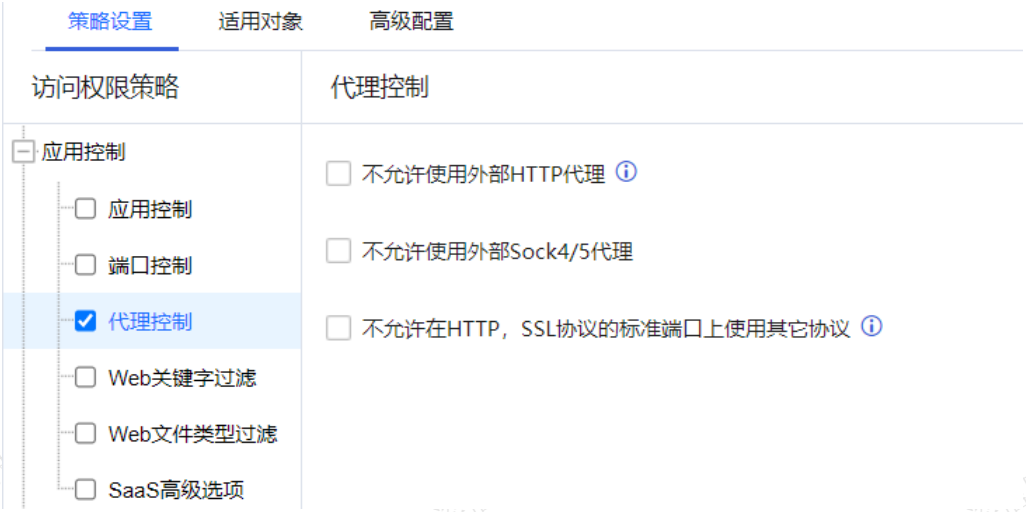
步骤9.选择适用对象和配置高级设置，点击<提交>完成配置。

步骤10.当用户去访问百度网页会被拒绝，打开CMD命令，查看访问网站的端口会出现连接失败。



代理控制

针对使用HTTP代理，SOCK代理和在HTTP协议与SSL协议标准端口使用其他协议的行为进行控制。



勾选[不允许使用外部HTTP代理]，则内网用户使用外网HTTP代理服务器方式上网时将被设备拒绝。

勾选[不允许使用外部Sock4/5代理]，则内网用户使用SOCK代理方式上网的行为将被设备拒绝。

勾选[不允许在HTTP，SSL协议的标准端口使用其他协议]，则对于那些已知/未知的软件通过常用知名端口（TCP80、TCP443）来通讯，但是通讯的内容是其私有协议格式时，这些通讯信息将被设备拒绝。

Web关键字过滤

Web关键字过滤功能是通过搜索引擎搜索词和HTTP上传两个部分进行过滤拒绝或告警。搜索引擎上搜索过滤关键字是通过百度、Google等搜索某些关键字。HTTP上传过滤关键字是通过HTTP协议上传关键字，如对论坛、QQ空间等发贴内容的关键字进行过滤或告警。

说明：

由于现在很多网站都是HTTPS协议，需要配合开启SSL解密才能识别文字和HTTP上传动作。

配置举例：设置一条全天拒绝搜索“求职”类关键字，允许搜索“游戏”类关键字，但是需要将搜索“游戏”类关键字的行为发告警邮件到sangfor@sangfor.com.cn，且禁止通过HTTP上传包含“深信服测试”敏感词汇关键字的数据的实例策略。

操作步骤

步骤1.在[行为管理/访问权限策略]，点击<新增>，选择[访问权限策略]，进入新策略编辑界面，勾选<启用该策略>，策略才会生效。

步骤2.填写策略名称和描述信息，其中策略名称为策略的唯一标识，不能重复，为必填项。描述信息是策略的概要，非必填项。

勾选<关键字过滤>，右边进入搜索引擎搜索词编辑页面。点击<添加>按钮，添加一条“暴力”，URL选择全部，动作拒绝；一条“游戏”，URL选择全部，动作为告警，生效时间均选择全天。

此处分别引用了关键字组和时间计划组。点击[关键字]下方的下拉按钮，选择需要处理的关键字组。

如果关键字组里没有包含需要的关键字，可以点击下拉框中的<新建关键字组>按钮，创建新的关键字组。

步骤3.选择<HTTP上传>进入编辑页面，点击<添加>按钮，进入HTTP上传添加界面。点击<添加>一条策略。点击[关键字]下方的下拉按钮，会列出关键字组列表。 新增一条敏感词汇组，关键字“深信服测试”；动作拒绝，生效时间为全天。

步骤4.点击<适用对象>，此处选中的用户/位置/终端类型/目标区域将全部匹配此上网策略设置的权限。

步骤5.点击<高级配置>，设置包括策略过期日期设置、同级别管理员查看编辑权限设置、允许低级别管理员查看；配置完成点击<提交>。

步骤6.由于当前很多网站都是使用HTTPS协议，因此需要开启解密策略才能过滤关键字信息，SSL解密策略的适用对象中需要包含过滤Web关键字过滤策略的对象，其详细配置请参考新增SSL解密策略章节。

步骤7.配置邮件告警需要设置开启Web关键字过滤告警，请到[系统管理/系统配置/告警选项/告警事件]，如下图所示。

步骤8.设置告警邮件的发送邮箱服务器地址和接收邮箱，配置路径在[系统管理/系统配置/告警选项/邮件告

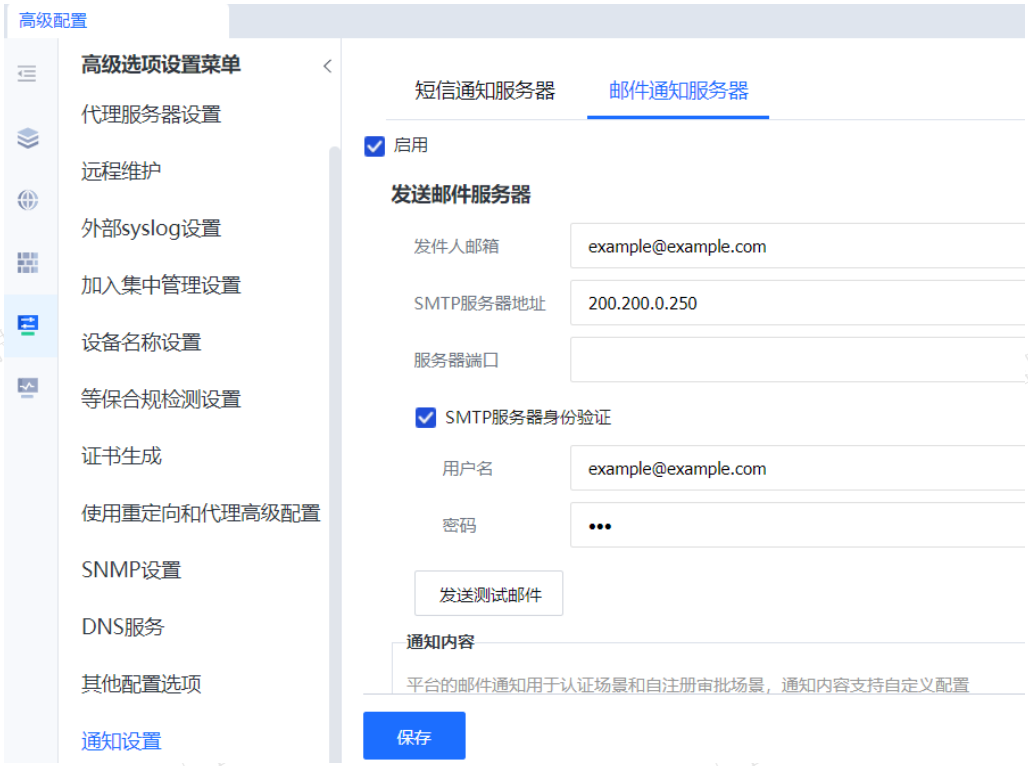
警]。先配置收件地址邮箱，确保该邮箱能正常接收邮件。

步骤9.例如配置QQ邮箱服务器，需要在[设置/账号]找到服务器配置方式，确保SMTP已开启。根据需求点击<如何使用 Foxmail 等软件收发邮件？>去获取STMP服务器地址和端口。

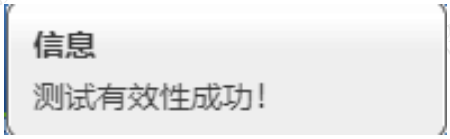
步骤10.点击<生成授权码>，跳转验证码发送页面，使用绑定邮箱的手机号发送短信到指定的号码，手机上发送成功，再点击<我已发送>。

步骤11.页面弹出生成授权码。

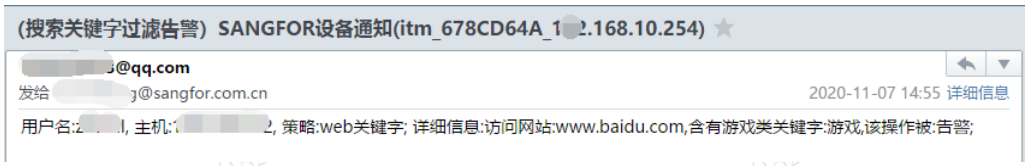
步骤12.点击<配置发送邮件服务器>跳转到邮件服务器通知页面。填写刚才配置的邮箱地址、SMTP服务器地址、服务器端口。STMP服务器验证填写的用户名与发件邮箱一致，密码为授权码。



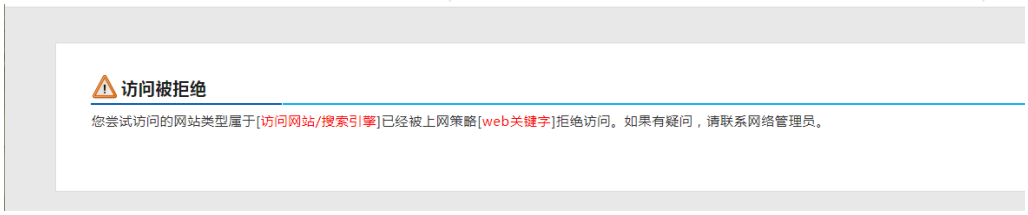
步骤13.点击<发送测试邮件>，输入能正常接收邮件的邮箱地址，发送成功后，页面会弹出“测试有效性成功”，说明配置的发送邮件服务器能正常发送邮件。点击<提交>邮件通知服务器配置完成。



步骤14.用户在浏览器访问含有“游戏”关键字。收件箱会收到告警邮件。



用户在浏览器访问“求职”关键字，会出现访问被拒绝的提示页面。



Web文件类型过滤

Web文件类型过滤功能是通过HTTP协议和FTP协议上传和下载的文件类型过滤。

说明：

1．其中FTP协议需要在页面勾选以下限制也适用于FTP上传和下载，如果不勾选策略仅在HTTP生效。

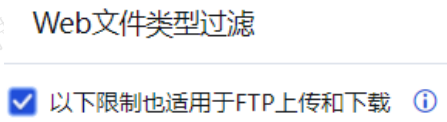
2．排除网站功能仅对HTTP上传和下载有效，对FTP请在[系统管理/系统配置/全局排除]中设置。

步骤1.在[行为管理/访问权限策略]，点击<新增>，选择[访问权限策略]，进入新策略编辑界面，勾选<启用该策略>，策略才会生效。

步骤2.填写策略名称和描述信息，其中策略名称为策略的唯一标识，不能重复，为必填项。描述信息是策略的概要，非必填项。

步骤3.勾选<Web文件类型过滤>，在Web文件类型过滤页面有上传和下载两种类型。

勾选[以下限制也适用于FTP上传和下载]选择，策略对FTP的上传下载起过滤作用。

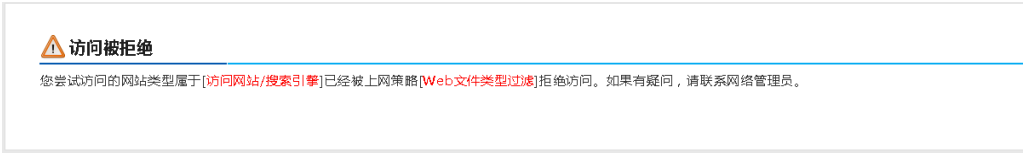


步骤4.设置文件过来类型，在上传页面点击<添加>按钮，选择拒绝的文件类型。例如选择“图片”、在下载页面点击<添加>按钮，选择拒绝的文件类型，例如选择“音乐”。动作选择拒绝，生效时间选择全天。

步骤5.如果还需要单独对某些网站的上传下载文件类型不做限制，则通过添加排除网站来实现。勾选<排除网站>，点击URL分类库，选择需要排除的网站URL分类。

步骤6.设置完成后，点击<提交>按钮，完成此策略的编辑。

步骤7.当用户在浏览器上传有关图片的文件和下载音乐文件时，页面提示访问被拒绝。



邮件过滤

邮件过滤功能用于对内网客户端通过SMTP、POP3协议发送的邮件进行过滤，过滤的条件可以设置收发邮件地址，邮件标题和正文的关键字等。

源地址过滤：是对发送邮件的发件人地址进行过滤。

• 勾选[不允许如下后缀的邮件地址发送邮件]，在窗口中输入需要过滤的邮件地址，当发件人匹配了这些地址，设备将不允许此邮件发送，反之没有匹配到则放通。

• 勾选[仅允许如下后缀的邮件地址发送邮件]，在窗口中输入需要放通的邮件地址，当发件人如果匹配了这些地址，设备将允许此邮件发送，反之没有匹配到则设备不允许此邮件发送。

目的地址过滤：是对发送邮件的接收人地址进行过滤。

• 勾选[不允许发送邮件到如下的邮件地址或如下后缀的邮件地址]：在窗口中输入需要过滤的邮件地址，当收件人如果匹配了这些地址，则设备将不允许此邮件发送，相反没有匹配到，则放通。

• 勾选[仅允许发送邮件到如下的邮件地址或如下后缀的邮件地址]在窗口中输入需要放通的邮件地址，那么邮件的收件人如果匹配了这些地址，则设备将允许此邮件发送，相反没有匹配到则设备不允许此邮件发送。

• [不允许发送标题和内容中包含有如下关键字的邮件]：检测发送邮件的标题和正文内容是否存在某些关键字，如果存在则不允许发送。比如过滤邮件标题或者内容中有求职关键字的邮件，在窗口中输入求职即可。

• [不允许发送带有如下类型附件的邮件]：检测发送邮件中所带附件的文件类型，如果匹配窗口中所填的类型，则不允许发送。

高级配置：

• 勾选[不发送超过如下大小的邮件]：启用对发送邮件的大小检测，如果超过设置值，则不允许发送。

• 勾选[不发送附件超过如下个数的邮件]，启用对发送邮件所带附件的个数检测，如果超过设置值，则不允许发送。

以上的设置是“或”关系，从上往下匹配，如果匹配到任意一项即执行放通或拒绝的动作，如果有冲突，以匹配到的第一条为准。

邮件过滤设置注意事项

1. [邮件过滤]中所有设置邮件地址的地方，既可以填写完整的邮箱地址，比如：xxx@abc.com，也可以填写邮件后缀，比如：@abc.com、abc.com。注意：填写abc.com，将同时匹配abc.com和abc.com.cn两种后缀的邮件。
2. [邮件过滤]中所有设置关键字的地方，支持正则表达式，比如key.*d，将匹配到keyd、keyword等。
3. [邮件过滤]是对使用SMTP协议发送的邮件进行过滤，对Webmail不生效，并且需要确保发送邮件的数据经过设备。发送邮件的SMTP协议标准端口是TCP25端口，如果发送邮件使用的是非标准端口，那么邮件过滤将对此类邮件不生效。
4. SMTP认证密码不能小于3个字符，如果SMTP认证密码小于3个字符的邮件审计后将发不出去。
5. [邮件过滤]开启邮件过滤时需要确保设备本身可以正常连接邮件服务器，否则邮件可能发不出去。
6. 保障邮件通知服务器可正常发送邮件。
7. 需要开启SSL内容识别功能，详细配置请参考新增SSL解密策略章节。

QQ号白名单

QQ号白名单用于设置对指定的QQ号进行放通，封堵其它QQ号码登录；支持PC和移动QQ应用。如果是以手机号、邮箱作为QQ账号是需填入腾讯自动分配的数字串账号。

操作步骤

步骤1.在[行为管理/访问权限策略]，点击<新增>，选择[访问权限策略]，进入新策略编辑界面，勾选<启用该策略>，策略才会生效。

步骤2.填写策略名称和描述信息，其中策略名称为策略的唯一标识，不能重复，为必填项。描述信息是策略的概要，非必填项。

步骤3.访问权限策略勾选<QQ白名单>，填写允许登录的QQ号。

步骤4.设置完成后，点击<提交>按钮，完成QQ号白名单配置。

步骤5.当用户用除了白名单列表中的账号登录QQ时，会出现登录超时的情况。

给特定的对象添加访问权限策略

上网对象和访问权限策略在设备上都是独立的元素，需要将它们关联起来访问策略才会起作用。查看设备的用户和给特定的用户添加权限策略的方法如下描述。

点击策略列表中的一条策略，在[策略设置/适用对象]中，可以看到策略可关联的上网对象，如下图。

对象包括四种类型：用户、位置、终端类型和目标区域。

用户：指用户的类型，包含所有用户、本地用户、用户属性组、源IP。

位置：通过不同的IP段、无线网络或VLAN三种方式划分不同的位置。

终端类型：指识别的类型：移动终端、PC、共享终端、IOT终端、医疗设备。

目标区域：指访问的目标IP范围。

说明
：

IOT终端和医疗设备适用于避免哑终端暴露在外网的风险并针对其做访问权限策略防止外联的场景。

其中用户类型的分类有：本地用户、域用户、域安全组、域属性、用户属性、源IP。

• 本地用户：是指同步到本地、认证策略添加到本地、本地创建的用户，这些用户可以直接在“本地用户”下进行选择。

• 域用户：中会以OU组的组织方式，列出已配置的所有LDAP服务器，可以在这里对OU或域用户进行选择。

• 域安全组：以OU组的组织方式，列出已配置的所有LDAP服务器，但是这里只能选择安全组，不能选择域用户以及OU组。

• 域属性：LDAP服务器上符合指定属性的用户。

• 源IP：内网用户的源IP范围。

在域属性页面，点击<新增>定义属性条件，一条规则可以设置最多5个条件，多个条件之间是“与”的关系。

“用户属性组”指符合指定属性的用户。在用户属性组页面，点击<新增>，定义属性条件，一条规则可以设置最多5个条件，多个条件之间是与的关系。

说明
：

1．用户类型下的本地用户、域用户、域安全组、域属性、用户属性组、源IP。它们的关系是“或”关系，而非“与”关系。例如选择了某个本地用户A以后，再选择某个域用户B，则策略是对本地用户A和域用户B都生效的。

2．这四种类型中，如果某个类型没有进行选择，那么这个类型将不会作为过滤条件，例如位置不进行配置，那么位置这个类型将不再作为条件过滤。

3．如果某条策略四种类型都没有进行配置，则这条策略是一条空策略，这条空策略只有策略内容，不关联任何用户，也不会对任何用户生效。

在用户管理中添加访问权限策略

步骤1.进入[接入管理/用户管理/本地组/用户]管理页面，在组织结构中选择需要添加策略的用户组如“工程师”。

步骤2.在右边[组织成员及权限策略设置]页面中点击<策略列表>。

步骤3.点击<添加策略>，选择需要关联的权限策略“工程师权限策略”，勾选[递归应用到子组]表示添加的策略同时关联给子组，不勾选则表示当前子组不会添加该策略，但当前组的直属用户以及后续新增子组默认会添加该策略。设置完成后点击<确定>。

步骤4.返回策略列表页面，查看用户组关联的策略列表。[应用于全部用户及子组用户]用于显示该策略是否被所有子组用户及直属用户引用。

在线用户管理中添加策略（需要单独对某个在线用户更改策略时）

步骤1.在[全网监控/入网用户管理/在线用户管理]页面，在在线用户列表中选择需要添加/编辑策略的用户“zuoml”。

步骤2.点击用户名，进入该用户编辑页面。

步骤3.在策略列表点击<添加策略>，选择需要关联的访问权限策略和审计策略。

步骤4.通过在线用户列表编辑和修改在线用户上网策略时，只能对非临时用户进行操作。如果是临时用户上线，点击在线用户列表中的用户名，只能查看该用户的策略结果集，无法在直接在在线用户列表中修改上网策略。

查看用户已匹配的策略

步骤1.在[接入管理/用户管理/本地组/用户]，查看本地用户、域用户策略配置的情况。

步骤2.点击用户组右边的<策略列表>，显示用户组关联的所有访问权限控制策略名称。

步骤3.点击<查看该组的策略结果集>，显示该组所有策略合并后的结果，如下图所示。

步骤4.[全网监控/入网用户管理]页面提供查看在线用户的访问权限策略的功能。

步骤5.点击需要查看上网策略的用户名，即可看到该用户匹配的上网策略。

说明：

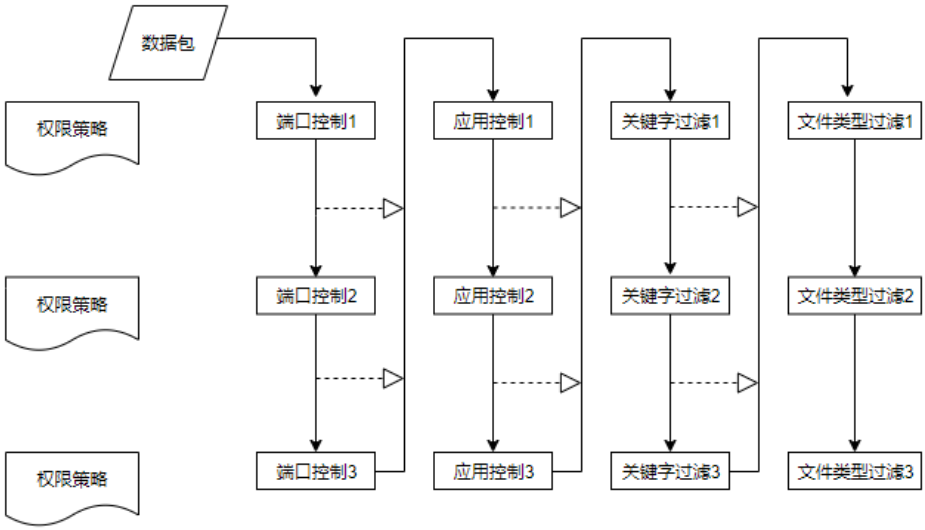
1．[接入管理/用户管理/本地组/用户]页面查看用户访问权限策略页面不会显示位置和终端的策略。

2．[系统管理/在线用户管理]页面查看的在线用户的访问权限策略，显示的是当前用户，当前位置，当前使用终端匹配的访问权限策略。

策略匹配说明

当用户/用户组同时关联了多条策略时，策略的匹配是有顺序的。访问权限策略中各种类型的策略按照匹配规则可以分两类：一类是支持多策略叠加的，此类策略从第一条往下逐条匹配，直至匹配到最后一条；另一类是不支持多策略叠加的，即设置会以第一条生效的为准，不会往下匹配。

支持多策略叠加的包括：应用控制、端口控制、Web关键字过滤、Web文件类型过滤、QQ号白名单、流量配额、时长配额、流速限制、并发连接数控制、准入策略、行为审计。访问权限策略的匹配顺序如下图所示。其他可叠加策略从上往下匹配。



不支持多策略叠加的包括：代理控制、SSL解密策略、邮件过滤、流量与上网时长审计、网页内容审计、公告页面、在线终端限制。这些策略以第一条生效的策略为准。

策略列表中将策略的顺序调整后，[行为管理/用户管理/本地组/用户/策略列表]中的策略顺序也会相应的调整顺序，保证所有的策略顺序都是一致的。

以模板新增策略

以模板新增策略：用已经做好的策略或系统内置的策略作为模板来新增一个策略。

新增的策略设置默认和模板是相同的，方便新增相同和相似的上网策略。设备内置的模板如下图所示。

比如当以[降低网络安全风险]为模板，新增一个策略。则新增的策略，会把模板策略的所有设置拷贝过来。您可以修改策略名称、描述信息、策略设置、适用组和用户、高级配置。

说明：

策略的高级配置中如果没有勾选[允许低级别管理员查看]，低级别管理员登录控制台后，无法以此策略做模板新增策略。

访问权限策略管理

在[行为管理/访问权限策略]，管理员可对访问权限策略对终端插件检查规则和流量行为检查规则进行删除操作、批量编辑、导入/导出等操作，组合规则仅支持删除和编辑操作。

表16访问权限策略管理说明

操作	功能说明
删除	在访问权限策略页面，选定一条策略，勾选需要删除，点击删除，设备会弹出一个操作确认框，点击<是>，则删除选中的规则。
编辑	在访问权限策略页面，点击检查规则名称，设备会弹出检策略的编辑页面，修改访问权限策略，根据需求进行修改。
批量编辑	批量编辑多条策略时只能统一编辑策略的[适用组和用户]选项，当您需要对某些用户组或者用户统一关联多条策略时可以使用此功能以方便操作。
导入/导出	用于把已经做好的策略导出做一个备份。在需要的时候把策略导入到系统中。如果有多台相同版本的设备，需要做相同的策略，也可以把做好的策略导入到另外的设备中，避免重复配置策略。
移动策略	用于调整策略对象的顺序，因为策略的执行是有先后顺序的，策略是由上往下执行的，通过上移或者下移策略来调整策略对象的优先级。
启用/禁用	启用表示策略为可用状态，调用该策略，策略里面所有设置的规则都会生效。 禁用表示策略为不可用状态，调用该策略，策略里面所有设置的规则都不生效。

终端防泄密

终端防泄密对用户使用应用程序或浏览器外发文件进行管控，通过敏感文件识别规则可以定义外发文件识别参数（文件类型、文件大小、文件名），精细化管控文件外发行为。

表17终端防泄密文件外发管控和访问权限策略对文件外发的区别

功能模块	准入客户端	生效方式	SSL解密	离线生效
访问权限策略	否（终端SSL解密除外）	基于流量	https及部分应用需要开启	否
终端防泄密	是	基于准入客户端	否	是

针对终端PC的应用和浏览器外发手段，主要包含4类通路：

1. 上传按钮：通过PC应用的上传按钮或文件选择框，打开windows本地的文件夹路径，选中文件或文件夹后外发。
2. 拖拽：从windows的本地文件夹中，选中要外发的文件或文件夹，以拖拽文件的方式进行外发。
3. 复制粘贴（剪贴板）：在windows的本地文件夹中，选中要外发的文件或文件夹，通过Ctrl＋C或右键复制，然后粘贴到PC应用的发送或编辑界面框中，进行文件或文件夹的外发。
4. 右键发送：安装PC应用后，部分应用具有选中windows桌面快捷方式图标，右键后会显示“发送到”的选项，故用户可通过右键发送的方式，选中要外发的文件或文件夹。

说明

“终端防泄密”功能模块的配置界面在设备未激活“防泄密外发管控授权”时处于隐藏状态。

文件外发管控

在[行为管理/终端防泄密/文件外发管控]，管理员可对文件外发管控策略进行新增、删除、批量编辑、启用/禁用、上移/下移、移动到、导入/导出、高级配置。

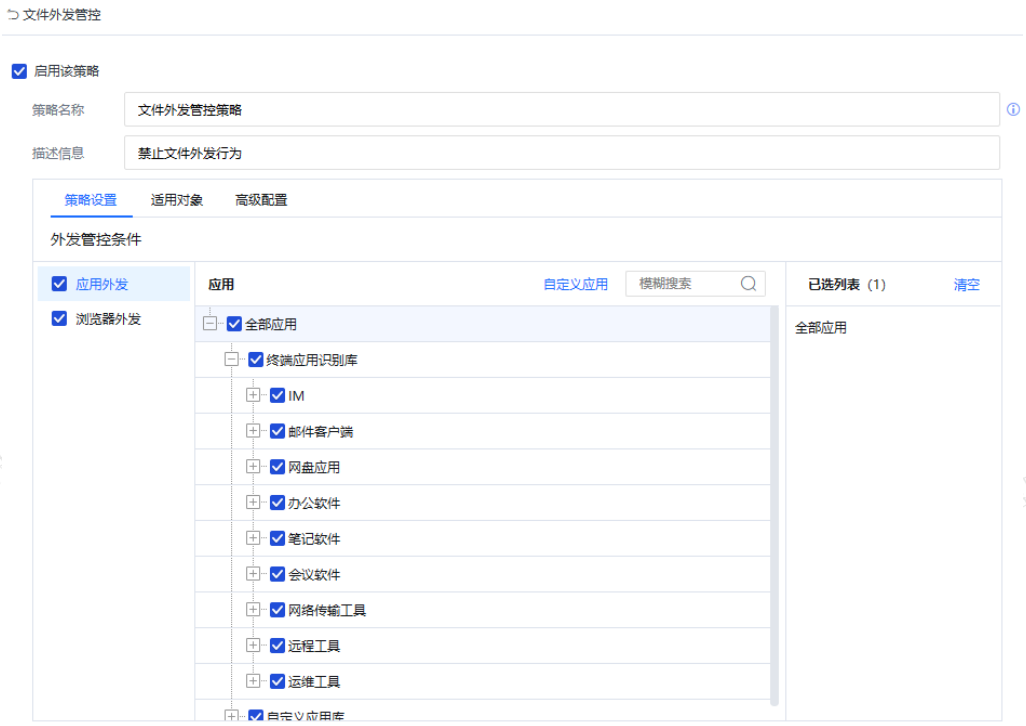
表18文件外发管控说明

操作	功能说明
新增	在文件外发管控页面，新增一条文件外发管控策略。
删除	在文件外发管控页面，选定一条策略，勾选需要删除，点击删除，设备会弹出一个操作确认框，点击<是>，则删除选中的规则。
批量编辑	批量编辑多条策略时只能统一编辑策略的[适用组和用户]选项，当您需要对某些用户组或者用户统一关联多条策略时可以使用此功能以方便操作。

启用/禁用	启用表示策略为可用状态，调用该策略，策略里面所有设置的规则都会生效。 禁用表示策略为不可用状态，调用该策略，策略里面所有设置的规则都不生效。
上移/下移	用于调整策略对象的顺序，因为策略的执行是有先后顺序的，策略是由上往下执行的，通过上移或者下移策略来调整策略对象的优先级。
移动到	用于调整策略对象的顺序，因为策略的执行是有先后顺序的，策略是由上往下执行的，通过移动到来调整策略对象的优先级。
导入/导出	用于把已经做好的策略导出做一个备份。在需要的时候把策略导入到系统中。如果有多台相同版本的设备，需要做相同的策略，也可以把做好的策略导入到另外的设备中，避免重复配置策略。
高级配置	用于配置准入客户端检测外发文件失效时的处置动作，该配置为全局配置，针对所有文件外发管控策略生效： 1. 文件检测失败：当文件检测失败时，允许文件外发/拒绝文件外发。 2. 文件检测超时：当检测时间超过[自定义]秒时：允许文件外发/拒绝文件外发。 3. 文件数量超限：当文件数量超过[自定义]个时：允许文件外发/拒绝文件外发。

新增访问权限策略

步骤1.在[行为管理/终端防泄密]点击<新增>一条文件外发管控策略。



策略名称：填写策略名称和描述信息，其中策略名称为策略的唯一标识，不能重复，为必填项。

描述信息：描述信息是策略的概要，非必填项。

策略设置：在策略设置选项卡中可以选择“应用外发”和“浏览器外发”。“应用外发”包含：内置终端应用识别库（IM、邮件客户端、网盘应用、办公软件、笔记软件、会议软件、网络传输工具、远程工具、运维工具）和自定义应用库（参考10.1.3.2. 自定义终端应用库章节）。浏览器类型包含：Google Chrome、Microsoft Edge、火狐浏览器、QQ浏览器、IE浏览器、搜狗浏览器、猎豹浏览器、遨游浏览器；URL名单：可以针对指定URL的外发行为进行管控。

适用对象：选中的用户/位置/终端类型/目标区域将全部匹配此上网策略设置的权限。

高级配置：包括策略过期日期设置、同级别管理员查看编辑权限设置、允许低级别管理员查看。

其中：

• 策略过期日期设置：是设置该策略的生效期。如果设置为[永不过期]，则策略将永久有效。如果设置[过期时期]，比如选择日期为2023-06-01，则表示此策略在2023-06-01之后过期，成为无效策略。

• 同级别管理员查看编辑权限设置：有两种权限可以选择[允许查看]和[允许编辑]。此处的“同级别管理员”指的是在[系统管理/系统配置/管理员账户]中属于同一角色的管理员，如果勾选[允许查看]，则同级别管理员可以查看此策略，而不能进行修改。如果勾选[允许编辑]，则同级别管理员默认拥有[允许查看]权限，并且可以对此策略进行修改。

• 允许低级管理员查看：勾选此项，则低级管理员可查看此策略，权限只限于查看，不能修改策略。“低级管理员”指的是在[系统管理/系统配置/管理员账户]中设置的角色级别低于建立此策略的管理员级别的管理员。

步骤2.在文件外发管控策略中配置敏感文件识别和处置动作，最后点击<提交>。

敏感文件识别：可以开启敏感文件识别，精细化匹配外发文件属性，如果没有开启，默认对所有文件属性类型进行管控。参考7.3.2. 敏感文件识别规则章节。

执行动作：可选择拒绝文件外发或允许文件外发；可选择是否开启终端提醒，右下角冒泡终端提醒；可选择是否开启外发文件存档，如拒绝文件外发后并存储在日志中心。

生效时间：可制定时间计划，使文件外发管控策略在指定时间段生效，默认全天。

离网管控：可选择开启离网继续生效，用户未连接AC设备时继续生效。

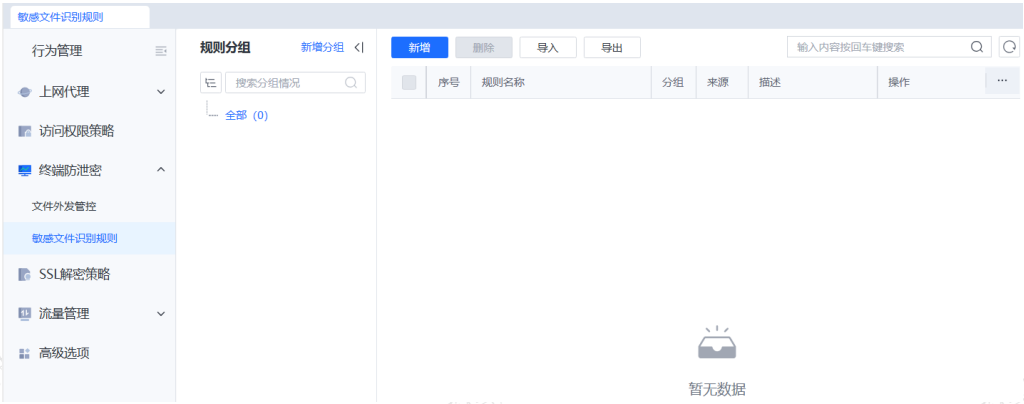
说明

在批量外发文件时，多个文件同时外发，会判定为一个文件属性。例：同时发送doc和txt文件，文件外发管控策略要同时放行doc和txt文件才允许外发；如果文件外发管控策略只拒绝doc，那么同时发送doc和txt都不能外发成功。

步骤3.配置完成后可在[行为管理/终端防泄密]查看文件外发管控策略。

敏感文件识别规则

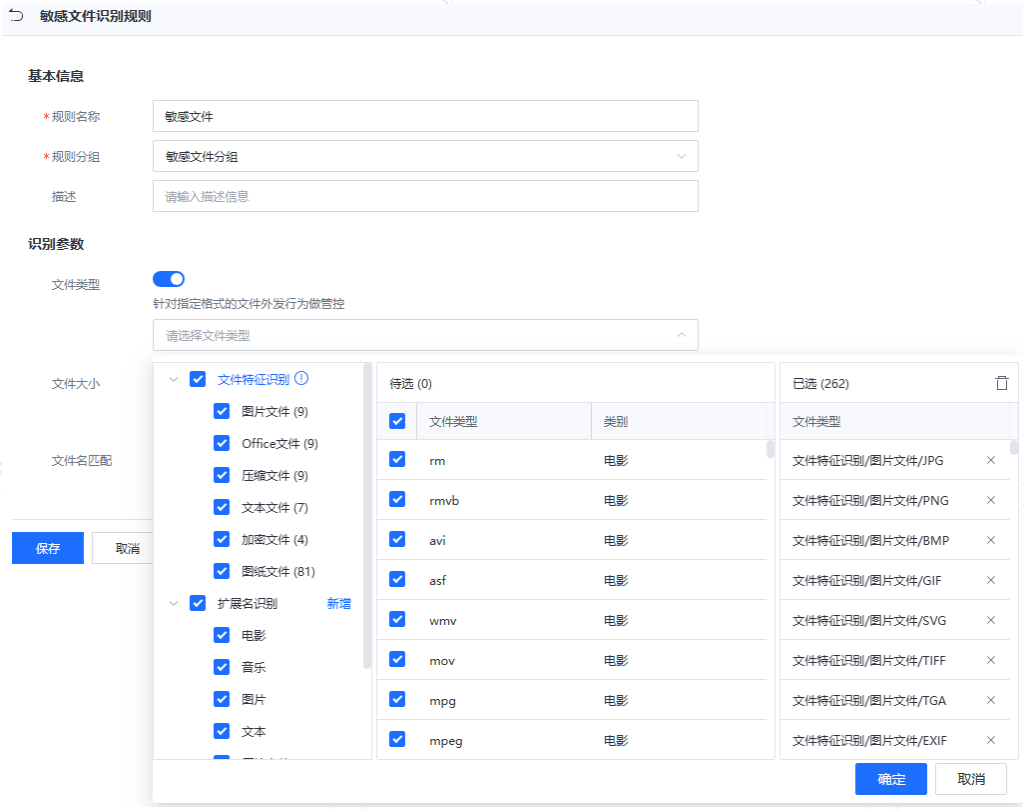
在[行为管理/终端防泄密/敏感文件识别规则]，管理员可以对敏感文件识别规则进行新增、删除、导入、导出，同时，也可以在规则分组中新增分组，对敏感文件识别规则进行分组。

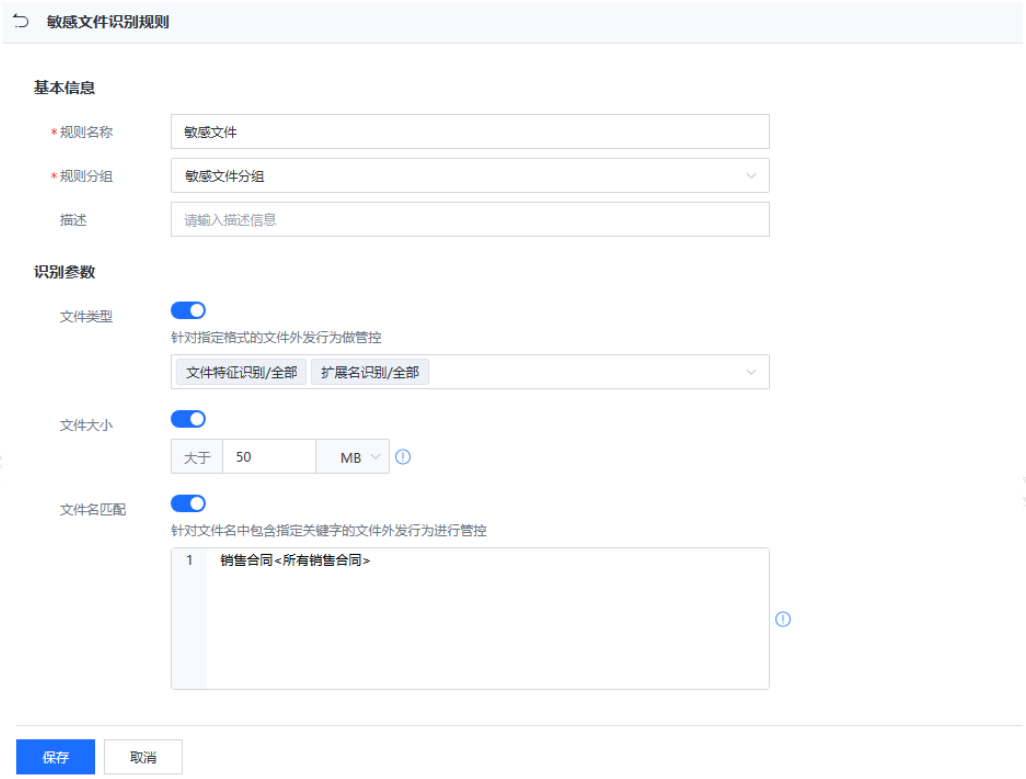


新增敏感文件识别规则

步骤1.在[行为管理/终端防泄密/敏感文件识别规则]点击新增分组，分组名称：敏感文件分组。

步骤2.在[行为管理/终端防泄密/敏感文件识别规则]点击<新增>敏感文件识别规则。





规则名称：定义敏感文件识别规则名称，其中规则名称为唯一标识，不能重复，为必填项。

规则分组：选择敏感文件识别规则所属规则组。

描述：描述信息是策略的概要，非必填项。

文件类型：包含文件特征识别和扩展名识别。文件特征识别，基于文件属性特征自动识别文件类型，可避免修改文件后缀导致管控策略被绕过的问题，由终端防泄密规则库更新；扩展名识别，根据文件后缀识别，可自定义新增。

文件大小：定义检测文件大小范围，默认大于50M，最大支持64G。

文件名匹配：可以根据文件名关键字进行过滤匹配。

文件外发管控策略案例

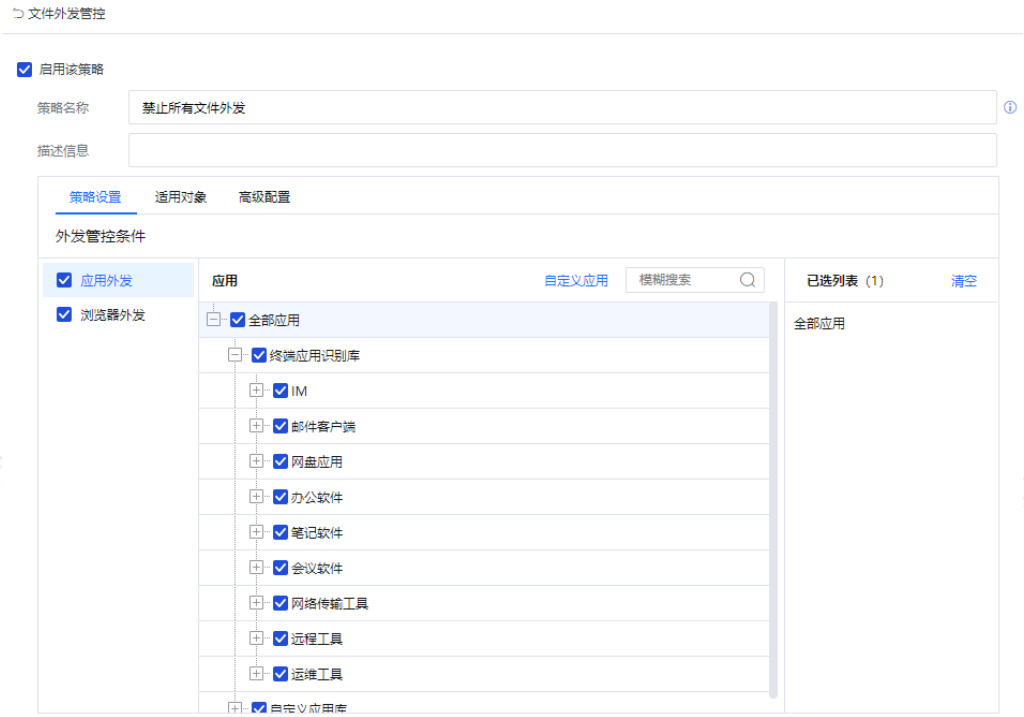
需求背景

某企业拥有许多重要的商业机密、专利等知识产权，为了防止这些重要信息被未经授权的人员获取或使用，希望对研发部严格管控文件的外发，禁止所有文件外发行为。

配置步骤

步骤1.AC设备完成部署模式、认证策略等基础配置（略）。

步骤2.在[行为管理/终端防泄密/文件外发管控/]新增文件外发管控策略，策略名称：禁止所有文件外发，在外发管控条件的应用外发选择全部应用；浏览器外发选择全部浏览器类型。



步骤3.在文件外发管控策略中的适用对象选择“研发部”。

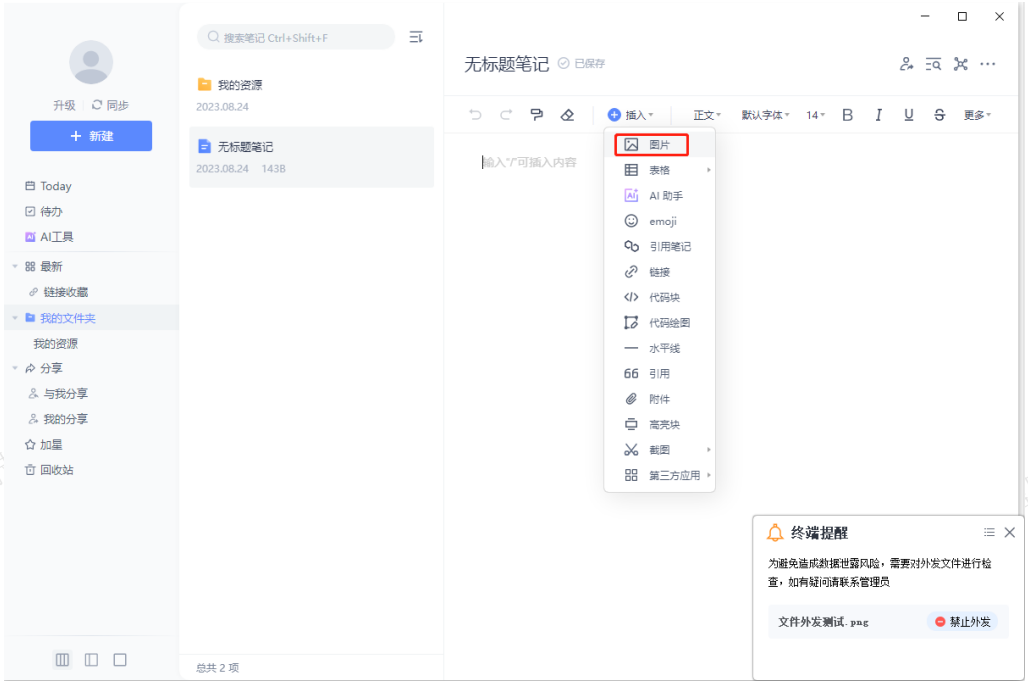
步骤4.在文件外发管控策略的处置动作中，执行动作：拒绝文件外发，开启终端提醒，开启外发文件存档；生效事件：全天；开启离网时继续生效。

效果呈现

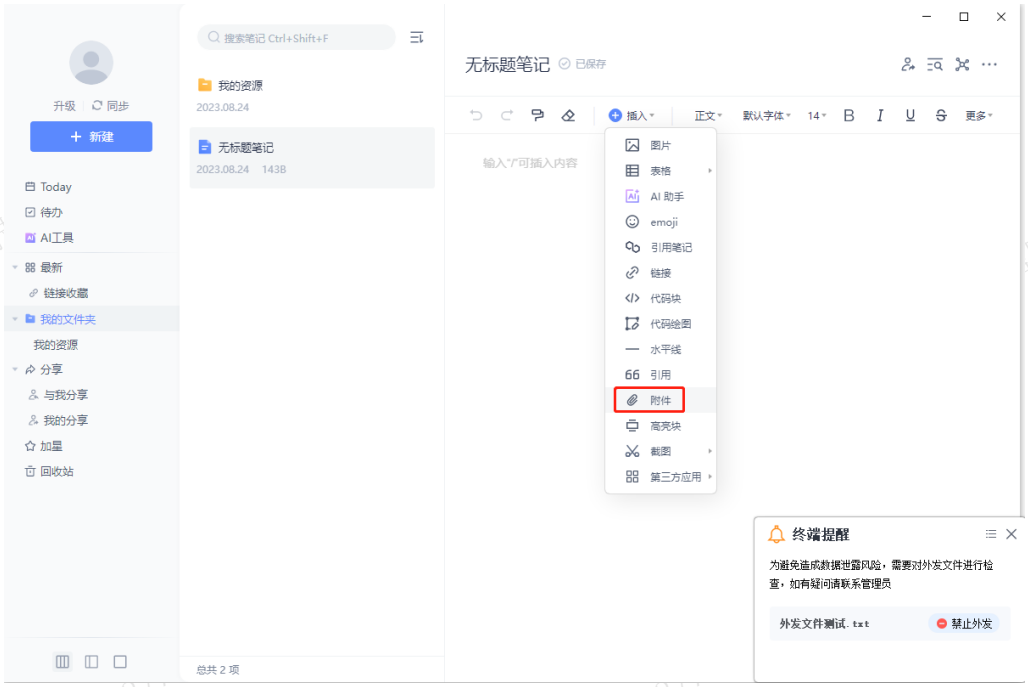
下以有道云笔记、谷歌浏览器外发文件为例

- 有道云笔记文件外发

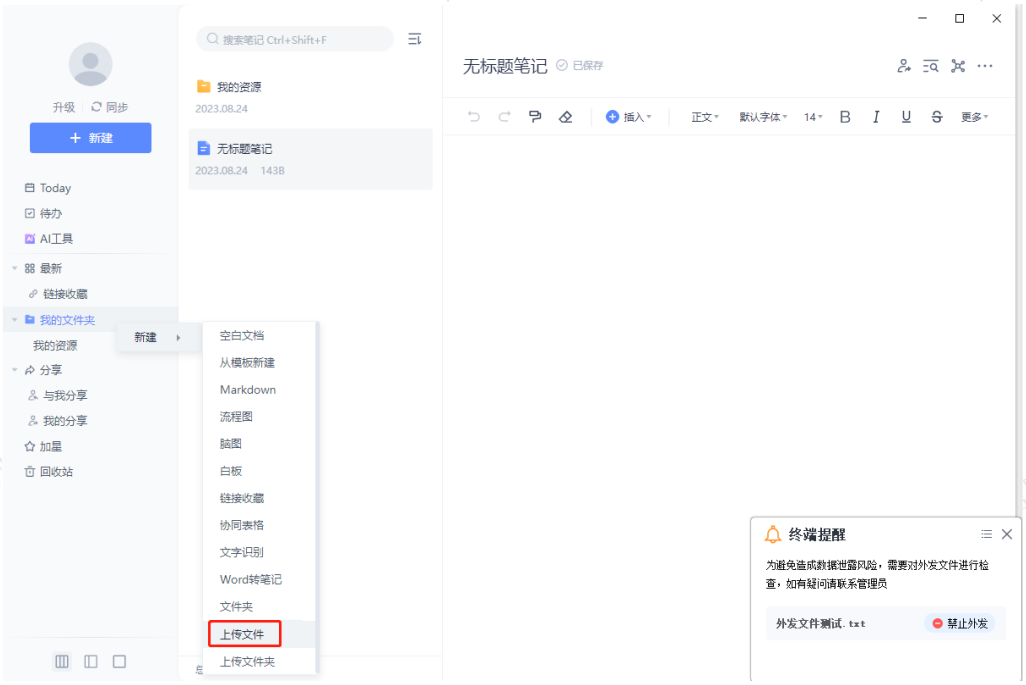
1. 在有道云笔记中无法插入图片，右下角显示终端提醒。



2. 在有道云笔记中无法插入附件，右下角显示终端提醒。



3. 在有道云笔记中无法上传文件，右下角显示终端提醒。



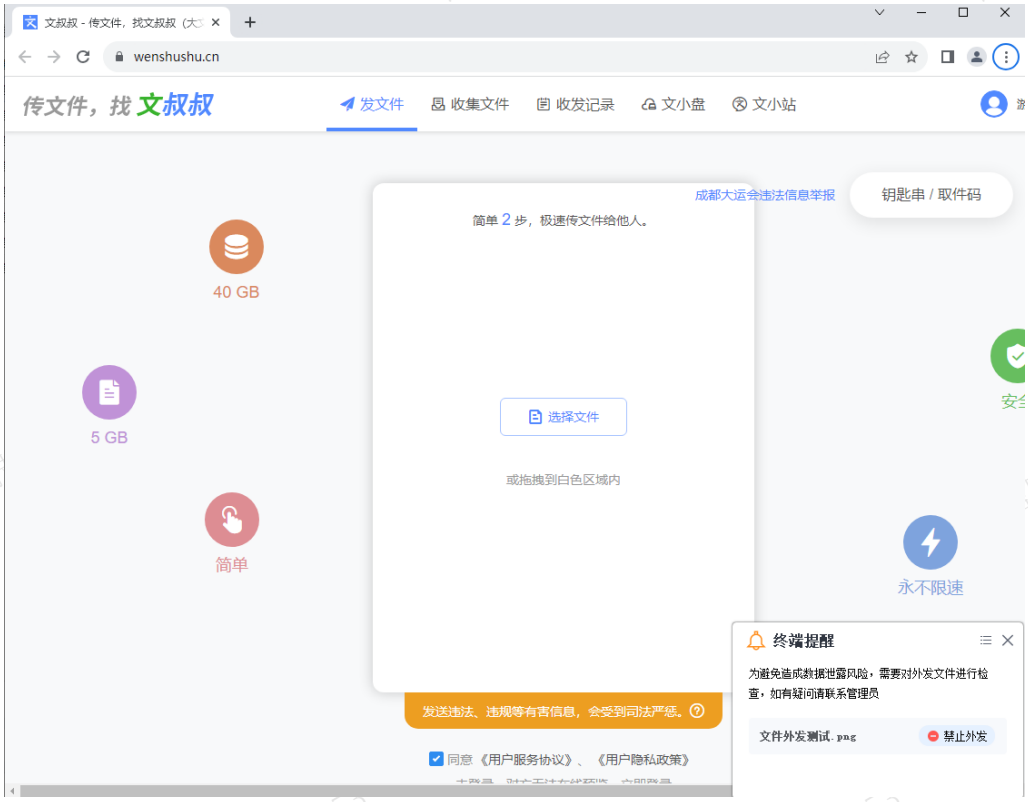
4. 在AC控制台[上网行为监控]可查看文件外发行为。

序号	发生时间	用户名	所属组	IP地址	应用类型	应用名称	动作	解密情况	详细信息
1	1分钟前	sangfor	/研发部	172.16.1.100	终端应用/笔记软件	有道云笔记	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zy1/Desktop/外发文件测试.txt 详细信息：通过笔记软件/有道云笔记外发
2	2分钟前	sangfor	/研发部	172.16.1.100	终端应用/笔记软件	有道云笔记	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zy1/Desktop/外发文件测试.txt 详细信息：通过笔记软件/有道云笔记外发
3	2.5分钟前	sangfor	/研发部	172.16.1.100	访问网站	搜索引擎	被记录	未解密	网站：safebrowsing.googleapis.com
4	2.5分钟前	sangfor	/研发部	172.16.1.100	终端应用/笔记软件	有道云笔记	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zy1/Desktop/文件外发测试.png 详细信息：通过笔记软件/有道云笔记外发
5	4分钟前	sangfor	/研发部	172.16.1.100	终端应用/笔记软件	有道云笔记	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zy1/Desktop/外发文件测试.txt 详细信息：通过笔记软件/有道云笔记外发
6	5.5分钟前	sangfor	/研发部	172.16.1.100	终端应用/笔记软件	有道云笔记	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zy1/Desktop/文件外发测试.png 详细信息：通过笔记软件/有道云笔记外发

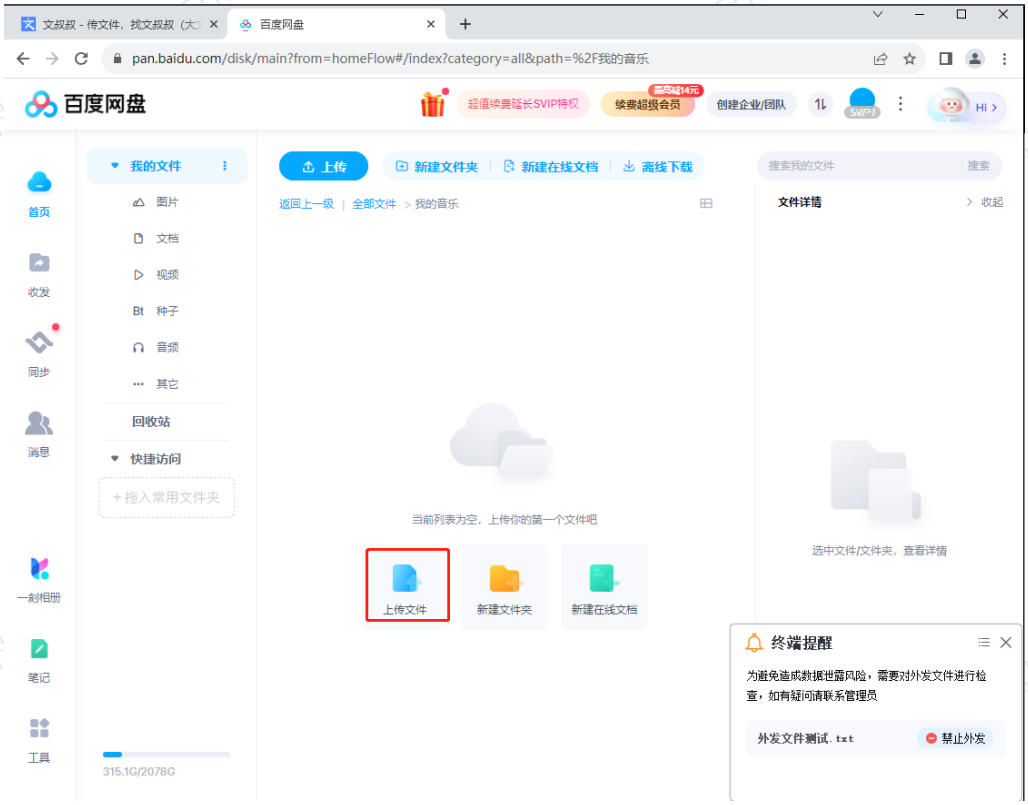
5. 在AC日志中心[日志查询/文件外发管控日志]可查看文件外发行为日志。

- **谷歌浏览器文件外发**

1. 使用谷歌浏览器访问“文叔叔”在线网盘，无法上传文件，右下角显示终端提醒。



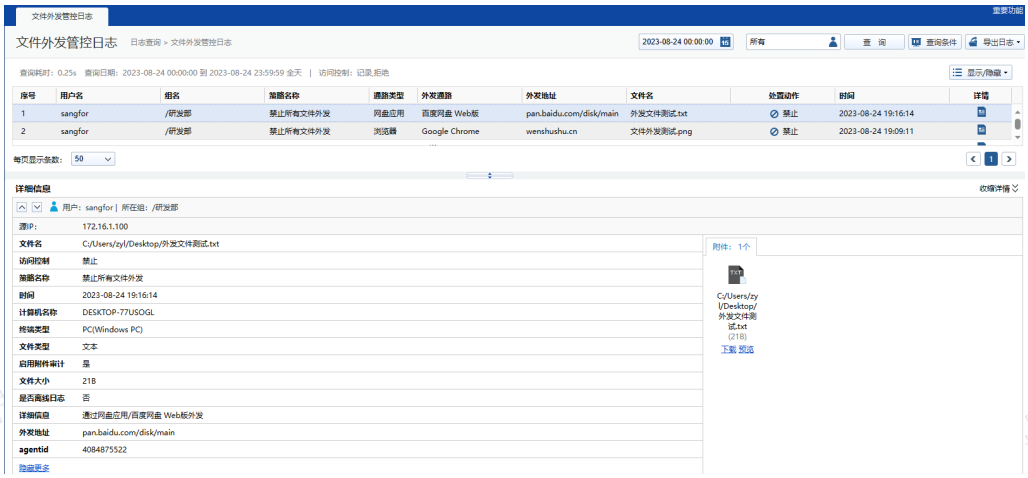
2. 使用谷歌浏览器访问“文叔叔”在线网盘，无法上传文件，右下角显示终端提醒。



3. 在AC控制台[上网行为监控]可查看文件外发行为。

序号	发生时间	用户名	所属组	IP地址	应用类型	应用名称	动作	解密情况	详细信息
1	1.5分钟前	sangfor	/研发部	172.16.1.100	终端应用/网盘应用	百度网盘 Web版	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zyl/Desktop/外发文件测试.txt 详细信息：通过网盘应用/百度网盘 Web版外发
2	8.5分钟前	sangfor	/研发部	172.16.1.100	终端应用/浏览器	Google Chrome	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zyl/Desktop/文件外发测试.png 详细信息：通过浏览器/Google Chrome外发
3	16分钟前	sangfor	/研发部	172.16.1.100	终端应用/笔记软件	有道云笔记	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zyl/Desktop/外发文件测试.txt 详细信息：通过笔记软件/有道云笔记外发
4	17分钟前	sangfor	/研发部	172.16.1.100	终端应用/笔记软件	有道云笔记	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zyl/Desktop/外发文件测试.txt 详细信息：通过笔记软件/有道云笔记外发
5	17.5分钟前	sangfor	/研发部	172.16.1.100	终端应用/笔记软件	有道云笔记	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zyl/Desktop/文件外发测试.png 详细信息：通过笔记软件/有道云笔记外发
6	19分钟前	sangfor	/研发部	172.16.1.100	终端应用/笔记软件	有道云笔记	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zyl/Desktop/外发文件测试.txt 详细信息：通过笔记软件/有道云笔记外发
7	20.5分钟前	sangfor	/研发部	172.16.1.100	终端应用/笔记软件	有道云笔记	拒绝	未解密	策略名称：禁止所有文件外发 文件名称：C:/Users/zyl/Desktop/文件外发测试.png 详细信息：通过笔记软件/有道云笔记外发

4. 在AC日志中心[日志查询/文件外发管控日志]可查看文件外发行为日志



SSL解密策略

SSL解密策略的作用是对使用SSL安全协议连接的应用，包括加密后的网站、webmail、web-bbs、POP3、IMAP、SMTP等进行内容审计识别，网上银行、在线支付等金融相关的网站除外。

两种解密方式：SSL中间人解密和准入客户端代理解密。选择准入客户端代理解密需要配置准入策略才能生效。

表19解密方式的区别说明表

	中间人代理解密	准入客户端代理解密
要求	无PC系统要求、需要安装证书	windows系统的用户、需安装客户端、需要安装证书
推送方式	1．AD域、桌管软件、准入客户端推送安装证书，用户无感知 2．未安装证书用户，访问网页时触发重定向到证书安装页面，引导下载证书安装工具	1．准入客户端静默安装，用户没有感知 2．AD域、桌管软件、准入客户端推送安装证书，用户无感知 3．未安装证书用户，访问网页时触发重定向到证书安装页面，引导下载安装工具
优点	无需安装客户端，无PC系统要求	无需消耗AC性能，审计内容更加丰富

注意	基于网页分类解密需要消耗更多CPU资源，建议自定义域名进行解密，以减少过多流量解密造成对性能下降。 有全解密需求可以使用带硬件加速卡的硬件型号设备，硬件加速卡解密性能相比软件解密性能提升一倍，具体型号可以联系深信服各区域办事处或深信服渠道合作伙伴进行了解。

表20SSL内容识别注意事项说明表

通用	HTTPS解密功能配置在自定义填写域名列表的情况下，域名列表中不支持IP地址。
	HTTPS解密功能在使用的时候需要在终端上安装设备证书到受信任的根证书颁发机构。
	HTTPS解密不支持QUIC协议。建议勾选“解密审计时，拒绝QUIC协议”。
	HTTPS解密功能与SSL VPN的Easy connect协议存在冲突，在开启了HTTPS解密功能的情况下，终端上如果需要使用Easy connect通过SSL VPN访问总部资源，需要在AC设备的SSL全局解密的排除列表中排除掉SSL VPN服务器地址，否则会出现连接中断问题。
	该功能需要开通[多功能项授权/SSL内容识别授权]。
	当SSL中间人解密和准入客户端代理解密同时配置时，策略列表从上往下匹配，仅匹配到的第一条生效。
	若终端为虚拟机，不建议使用准入客户端代理解密，可使用SSL中间人解密。
客户端	当开启需要PC安装准入客户端，目前只支持Windows系统（XP系统不支持）。Mac系统和Linux系统可使用SSL中间人进行解密。
	代理客户端默认只对443端口进行解密。
	客户端的证书和SSL内容识别的证书是不同的证书。
中间人解密	HTTPS解密支持设备本身做代理的场景，但是只支持HTTPS代理、不支持SOCKS代理，客户端解密方案不支持在代理场景使用。
	存在证书双向校验的场景下，不能使用HTTPS解密功能，否则会存在客户端校验失败导致连接出错问题。
	如果终端的DNS请求数据不经过设备或者终端访问的HTTPS网站是直接以IP地址进行访问的，则不支持HTTPS解密功能。

操作步骤

步骤1.在[行为管理/访问权限策略]，点击新增<SSL解密策略>，点击启用该策略。

步骤2.填写策略名称、描述信息，策略名称是唯一的必填项，描述信息非必填项。

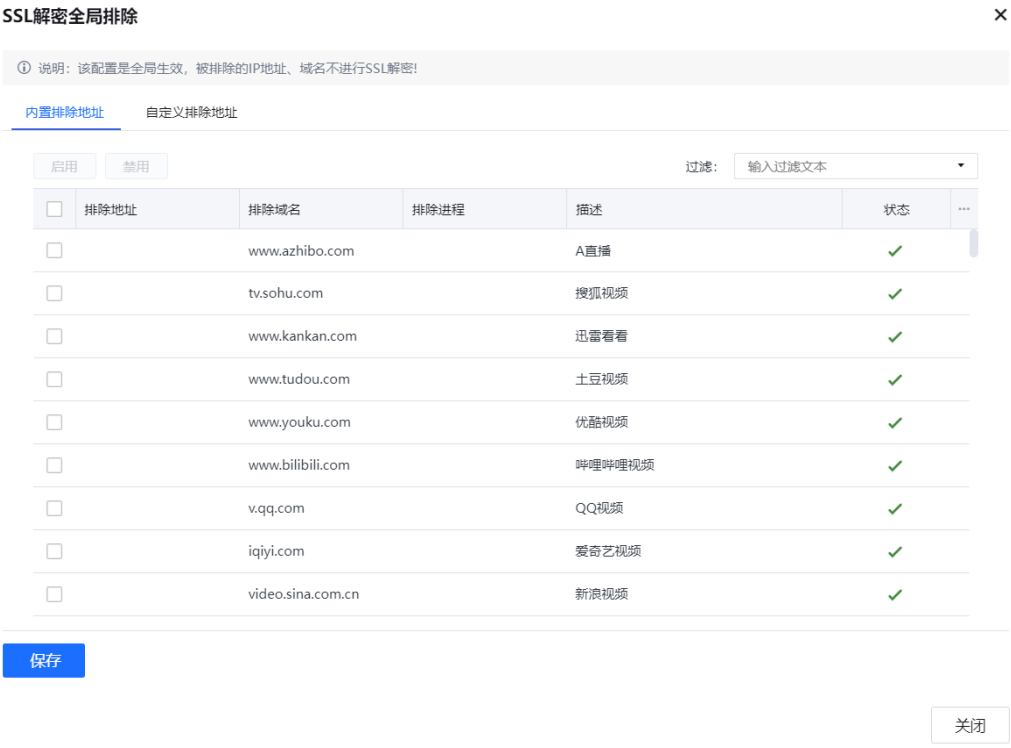
步骤3.解密方式可根据实际情况选择SSL中间人解密或者准入客户端代理解密。使用说明参考解密方式区别说明表。

步骤4.定义解密范围，勾选<加密web应用内容识别>，可选全部或者自定义两种方式进行配置，web应用仅支持识别使用443端口。

步骤5.选择自定义内容识别时，点击 可根据需求对SaaS应用或网页分类进行勾选。

步骤6.勾选“解密审计时，拒绝QUIC协议”，SSL解密不对QUIC协议的域名生效。

步骤7.点击<全局解密排除>，配置不需要做SSL内容识别的IP、域名、进程。三者是相与的关系，可灵活搭配使用。



步骤8.当需要识别邮件的25、465、143、993、587端口的内容时，需要开启邮件内容识别。

步骤9.[点击下载SSL识别根证书]，将下载的根证书安装到电脑上面，消除由于启用SSL内容识别带来的浏览器安全告警。如果在AD域环境下需要消除浏览器的安全告警，点击[AD域环境下解除终端浏览器告警的方法]，详细内容参考文档中的配置步骤。

步骤10.设置完成后，点击<提交>按钮，完成此策略的编辑，如果您还需要编辑其他类型的策略，则继续选择其他控制类型进行编辑。

说明：

1．SSL内容识别对网上银行、在线支付等金融相关无效。为防止敏感金融信息被审计到，设备中对此类信息做了屏蔽。

2.https场景要配置SSL内容识别。

流量管理

流量管理模块可以针对不同用户或者不同应用的所产生的网络流量做管理。该模块为企业提供了“带宽保证”和“带宽限制”功能，通过“带宽保证”功能可以保证企业重要应用的带宽，从而确保企业关键业务的持续性和高效性。而带宽限制功能可以基于不同的用户角色（例如：所有用户、本地用户、域用户、域内安全组、域内属性、本地用户属性组、源IP）、终端上线位置、终端类型以及目标区域等条件限制终端上下行总带宽或是某类应用的带宽。

流量管理概述

在[流量管理/流控策略/带宽分配]路径下提供了流量子通道的功能，企业可以根据需求新建通道，对通道内

的流量做更细致的管控。通过流量管理可以实现的主要功能有：

1. 动态保证企业重要业务应用的带宽，确保关键业务的持续性和高效性；

2. 限制网络应用的带宽；

3. 可基于IP地址、用户名来控制最大的带宽；

4. 通道内不同IP间带宽平均分配；

• 流量通道：在某条线路上将整个线路带宽按百分比分割为若干份，根据应用类型或者用户组来分配不同比例的带宽资源。根据流量通道的作用可以分为：带宽保证通道和带宽限制通道。

• 带宽限制通道：对通道的最大流速进行设置。网络繁忙时，该通道占用带宽不会超过设置的最大带宽值。

• 带宽保证通道：不仅设置此通道的最大带宽，而且设置最小带宽。当网络繁忙时，保证该通道的带宽不低于设置的最小带宽值。

• 流量子通道：必须指定某个流量一级通道才能划分流量子通道。流量子通道是对流量一级通道更细致的划分，可以对带宽做更细化的管理。

• 惩罚通道：与[用户限额策略]配合设置，在[用户限额策略]配置单用户所能够使用的应用流量额度并调用相应的惩罚通道，当用户使用超额流量后则会触发惩罚通道的配置进行处罚，惩罚通道的带宽根据实际需求设置，用户超额后就会被限制。

• 线路带宽配置：用于配置公网线路的实际上、下行带宽，设备网桥模式部署时，设置前置网关公网线路的实际带宽，因为限制通道和保证通道的带宽设置都是根据线路带宽来设置百分比，需要在线路带宽配置处设置和实际相符的线路带宽值。

• 虚拟线路：当设备以网桥模式部署时，可以通过[虚拟线路]功能将一条物理线路虚拟成多条线路或将多条物理线路虚拟成一条线路，针对虚拟出的线路进行流量管理。

流量通道匹配规则

勾选<启用流量管理系统>后：当数据经过设备时会以数据相关的信息作为条件，匹配已设置的流量通道。匹配的条件包括：用户组/用户、IP地址、应用类型、数据经过AC的时间、目标IP组。当数据包的所有条件与某条流量通道设置的值相匹配时，则该条流量通道就会对此数据生效。

流量通道的匹配顺序是从上往下匹配，同一个数据包只会匹配到一条流量通道，所以配置时需要把条件更加细致的通道放在上面。流量子通道的匹配顺序也是从上往下匹配，当数据匹配到父通道时不会立即执行父通道的策略，而是会继续从上往下检查有无匹配子通道，直达匹配上一条子通道策略就不会再往下检查。

流量管理功能管理

进入导航菜单栏[流量管理/流控策略]，如下图所示。

表21流量管理功能说明

操作	功能说明

启用流量管理系统	流量管理模块的总开关。不勾选则流量管理模块配置不生效。
高级配置	用于设置线路空闲阈值和设置是否启用线路繁忙保护功能。
编辑线路带宽属性	用于设置公网线路带宽。
带宽分配	用于设置管理保证通道、限制通道、惩罚通道。
编辑	选定一条通道，点击编辑，对该通道进行编辑修改。
删除	选定一条通道，点击删除，从列表里删除该通道。
启用/禁用	选定一条处于禁用状态的通道，点击启用使其生效；选定一条处于启用状态的通道，点击禁用使其不生效。
上移/下移/移动到	选定一条流量通道，点击上移将该通道位置上移，点击下移将该通道位置下移。点击移动到指定的位置。（与匹配规则有关）
线路筛选	当存在多条线路时，用于筛选列表显示的生效线路的通道策略。可以选择所有线路或者某条线路。
	左边图标为全部展开，展开所有一级通道下的子通道；右边图标为全部收起，收起所有子通道，只显示一级通道。（用于多子通道场景）

流控策略

流控策略通过对各种网络流量进行精细化控制和调度，使有限的带宽资源得到充分的利用。包括保证通道、限制通道、流量子通道、排除策略、惩罚通道等模块。支持AC路由模式和网桥模式部署时使用。

保证通道

用于保证重要应用的使用，通过设置最小带宽值，保证特定类型的数据占用带宽不小于某个值，从而保证在线路比较繁忙的时候，重要应用有足够带宽能正常使用。

需求场景

某公司租用了一条20Mbps电信线路，内网有1000名上网用户。根据公司业务需求，要保证财务部在访问网上银行网站和收发邮件的数据时，在线路繁忙时所拥有的带宽不能小于2Mbps，但最大不能超过5Mbps。

操作步骤

一、**配置保证通道**

步骤1.进入[流量管理/虚拟线路配置]配置公网线路带宽，点击<线路1>，在弹出线路配置窗口里，将[上行]、[下行]分别设置成20 Mbps。

步骤2.进入[流量管理/流控策略]，勾选<启用流量管理系统>，激活流量管理系统。[线路带宽]中显示各条公网线路的总带宽（本案例中用户只有一条出口链路，因此只有一条线路）。

步骤3. 在[带宽分配]中点击<新增通道>，选择<新增一级通道>，在弹出的[新增一级通道]页面，勾选<启用通道>。在[通道名称]中输入该通道的名称，[所属通道]用于显示通道级别，“/”表示此通道是一级通道。

二、带宽通道设置

在[通道编辑]中选择[带宽通道设置]，在右侧的[带宽通道设置]栏中设置通道的相关属性。

• 带宽通道设置：用于设置生效线路、带宽通道类型、限制或保证的带宽、单个用户所能使用的带宽等。

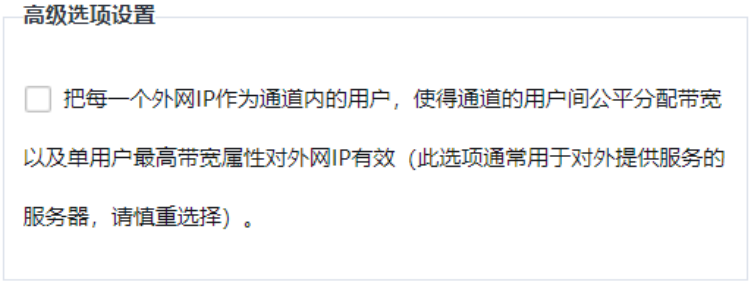
• 生效线路：用于选择通道适用的线路，也就是当数据走选中的线路时才会匹配到此通道。此例中只有一条线路，所以[生效线路]选择<线路1>。

• 带宽通道类型：用于选择通道类型（保证通道或者限制通道）并定义带宽值。此例中需要对财务部人员的访问网上银行类别的网站以及收发邮件的数据做带宽保证，保证至少2Mbps，最高不超过5Mbps，则此处勾选[保证通道]，设置[上行带宽]、[下行带宽]的[保证]和[最大]分别为20%和50%的总带宽，总带宽是20Mbps，则保证带宽为2Mbps，最大带宽为5Mbps。

• 优先级：分为高、中、低三类，指其他通道空闲时此通道占用空闲带宽的优先级。

• 启用限制单用户最大带宽：用于限制匹配到此通道的单个用户占用的带宽值。在此例中不需要对单个用户做最大带宽的限制，所以此处不勾选。

• 高级选项设置：勾选此项表示把每一个外网IP作为通道内的用户，使得通道的用户间公平分配带宽以及单用户最高带宽属性对外网IP有效（此选项通常用于对外提供服务的服务器，请慎重选择）。



三、通道使用范围

步骤1.在[通道编辑]中选择[通道使用范围]，在[通道使用范围]栏中设置通道适用的应用与对象用户。本例

中是对财务部人员的访问网上银行类别的网站以及收发邮件的数据做带宽保证，因此适用应用和适用对象都需要做自定义。

步骤2.自定义通道适用的应用。勾选[适用应用]栏<自定义>。(勾选<所有应用>则表示该通道针对所有类型的数据都生效)。

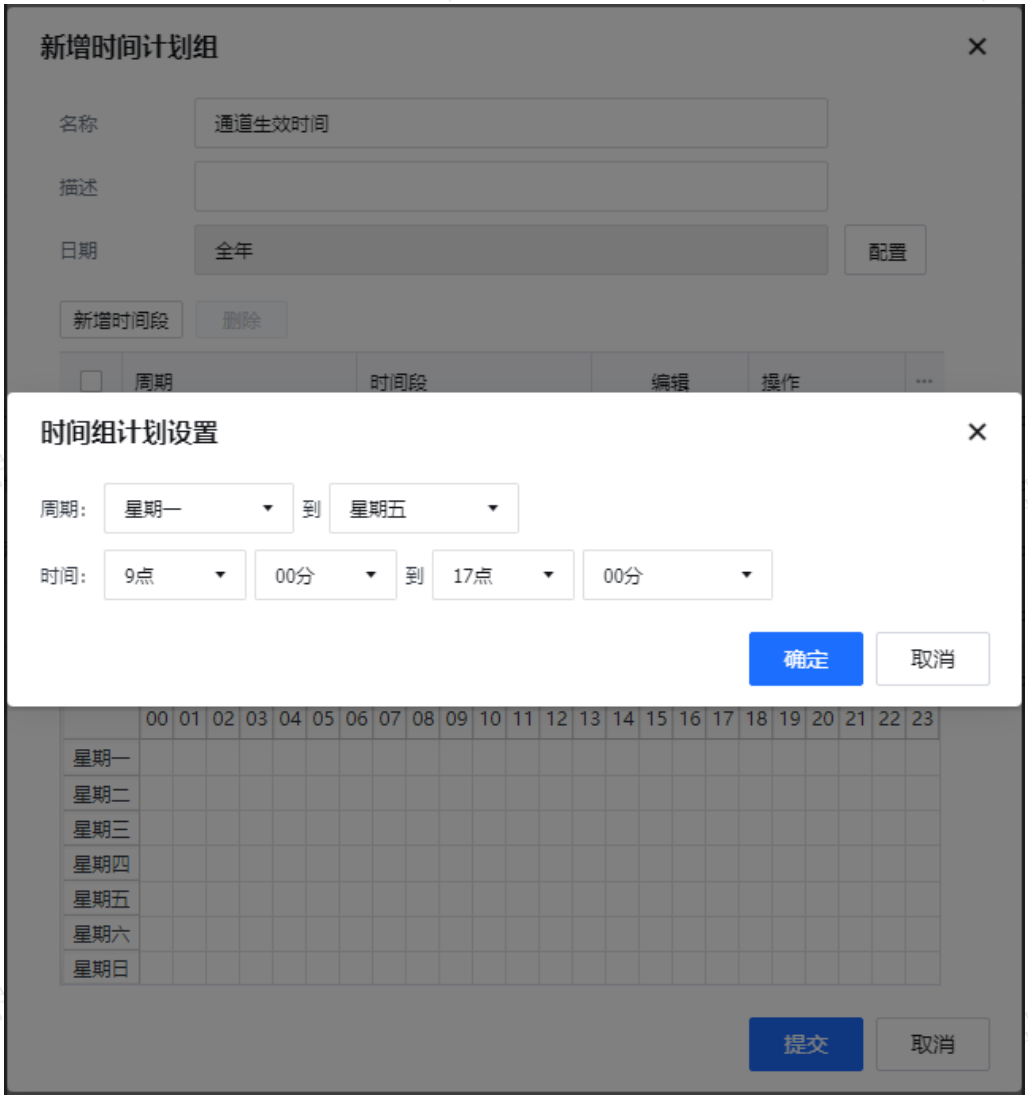
步骤3.点击<请选择>勾选特定的应用类型。在弹出框[自定义适用服务与应用]中选择应用类型和网站类型。

该案例需要访问网上银行类别的网站以及收发邮件的数据做带宽保证，则此处选择应用：邮件/全部、网上银行/全部、访问网站/金融/网上支付、访问网站/金融/银行网站。

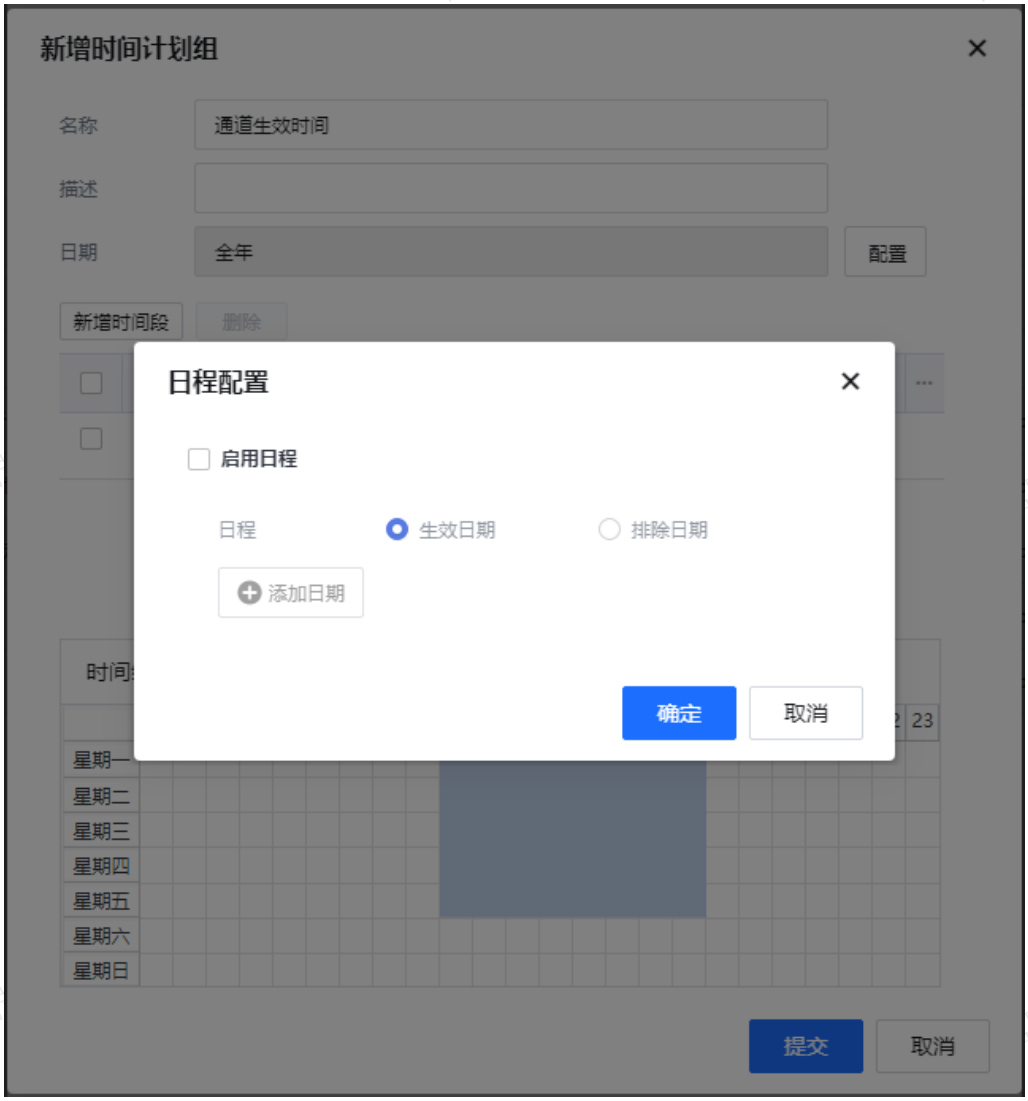
步骤4.自定义通道适用对象。勾选[适用对象]栏右侧的<自定义>。(勾选<所有用户>则表示该通道针对所有用户均生效)。

步骤5.点击蓝色字体<用户>按钮，在弹出框[自定义适用对象]中选择指定对象。本次例中需要对财务部的所有用户做带宽保证，则此处选择<财务部门>用户组，选择好[适用对象]后，点击<确定>完成设置。

步骤6.在[生效时间]栏内配置通道生效时间段，管理员可以视企业工作时间自定义生效时间段。在[生效时间]栏内点击<新增时间计划组>开始自定义策略生效时间段，点击<新增时间段>添加执行通道的时间。

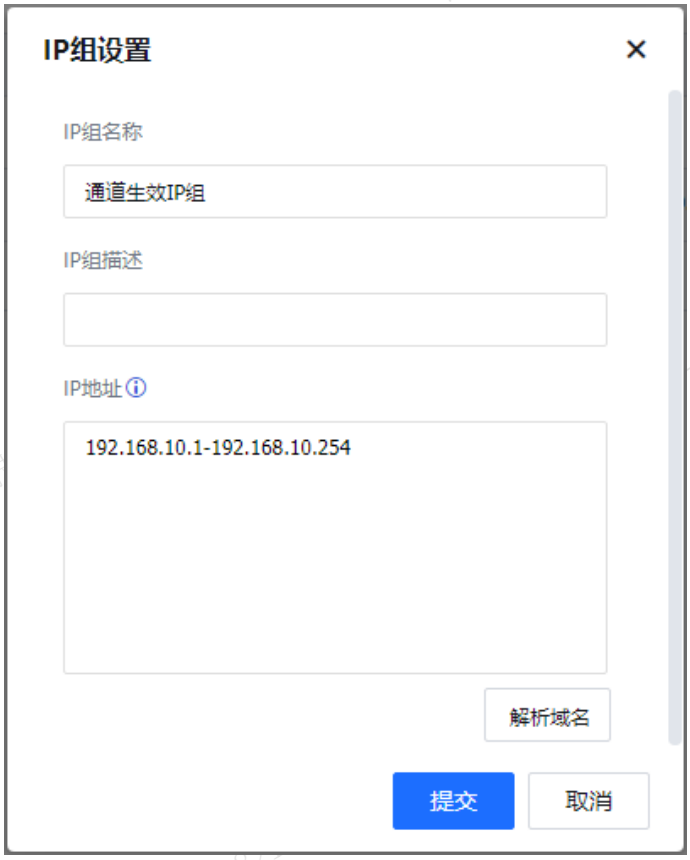


步骤7.如果预设置通道生效日期，则点击[日期]栏后的配置按钮，添加计划时间段或者排除时间段。设置完成后点击<确认>按钮，最后点击<提交>。



步骤8.配置策略的[目标IP组]，可以结合前文[通道使用范围]里的[适用对象]来使用。在本次案例中：在[适用对象]里已设置通道对财务人员生效，因此在此处可以将[目标IP组]定义为全部。

如果需要针对IP做更精细的限制，则可以自定义IP地址段。在[目标IP组]栏点击<新增IP组>。然后在弹出的[新增IP组]菜单下自定义通道生效的IP地址段。



设置完成后，显示如下。

步骤9.设置完成后，点击<确认>，完成保证通道的设置。点击确定保存后，看到提示信息后，点击关闭，完成配置。

步骤10.[带宽分配]中会出现设置的通道。保证通道配置完成。

说明

：

1．保证带宽通道百分比之和可能会超过100%时，当超过100%时，各保证通道的最小带宽值会按照比例进行缩减。比如，我们设置两条通道，第一条保证带宽设为30%，第二条设为90%，则第一条实际分配到30/（90+30）%，即25%，第一条实际分配到90/（90+30）%，即75%。

2．优先级：当我们的实际带宽有空余，优先级越高，越先占用空闲带宽。

限制通道

限制通道用于设置流量通道的最大带宽，对匹配到此限制通道的数据进行流量控制，控制此部分流量所能占用的最大带宽值。

需求场景

公司租用了一条10Mb/s电信线路，内网有1000名上网用户，发现很多市场部人员经常使用迅雷下载，P2P等下载工具进行下载，占用了大部分带宽，影响了其他部门的正常的办公业务，公司希望通过流量管理系统将市场部的这部分数据占用的带宽限制在2Mbps之内，并且每个用户这部分数据的占用带宽限制在30Kbps。

操作步骤

一、配置限制通道

本例中是对公司市场部人员使用迅雷下载、P2P等下载流量做限制。

步骤1.在[带宽分配/新增通道/新增一级通道]，在弹出的[新增一级通道]页面勾选[启用通道]。在[通道名称]中输入该通道的名称，[所属通道]用于显示通道级别，“/”表示此通道是一级通道。（不勾选该通道则为禁用状态，通道配置暂时不生效。）

步骤2.在[新增一级通道]的[带宽通道设置]栏勾选[限制通道]，在[上行带宽]和[下行带宽]中设置最大为20%（本示例中为2Mbps）。为了能够对每个用户的P2P下载流量做限制，还需要勾选[启用限制单用户最大带宽]并在按照需求在[上行]、[下行]中填写最大带宽值（本示例中为30Kbps）。在[优先级]选择低优先级。

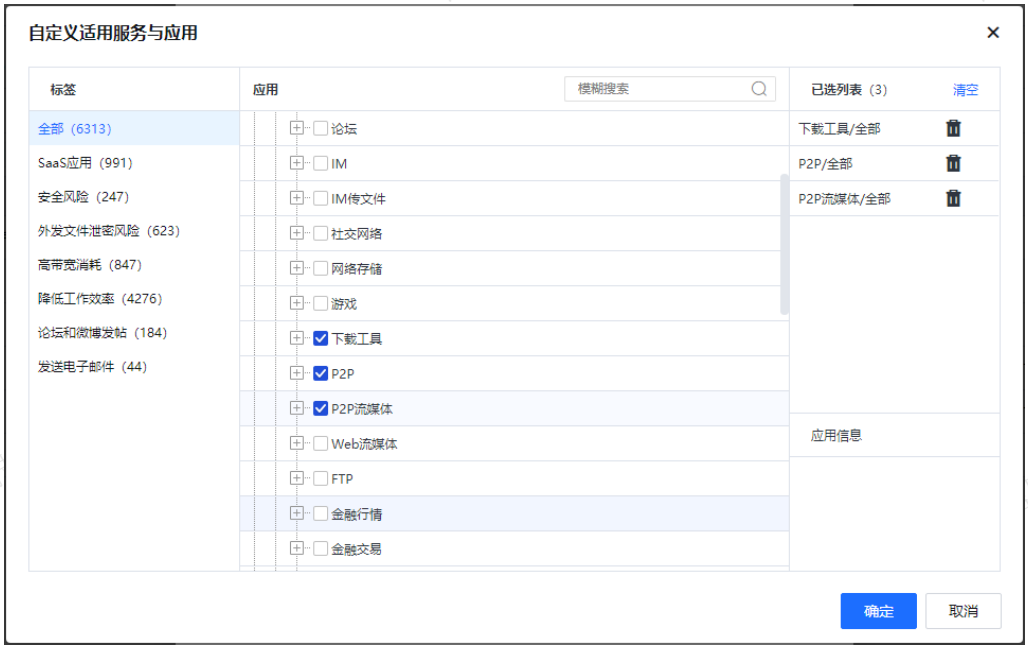
步骤3.勾选[抑制P2P下行丢包]选项。本条限制通道目的是限制P2P下载流量，通常P2P下载、流媒体等应用程序具备强烈的带宽侵占特性，导致设备在下行方向接收到的流量大于设定的最大带宽，这部分超过最大设置的数据包将被流量管理系统丢弃，而这部分丢弃的数据包实际上已经占用了线路的带宽，导致带宽浪费以及下行方向的拥塞。因此建议用户在对P2P流量做限制时勾选[抑制P2P下行丢包]选项，抑制P2P下载、流媒体等应用在下行方向的丢包率。

二、通道使用范围

本例中是对市场部人员的迅雷下载、P2P应用的流量做限制，因此适用应用和适用对象都需要做自定义。

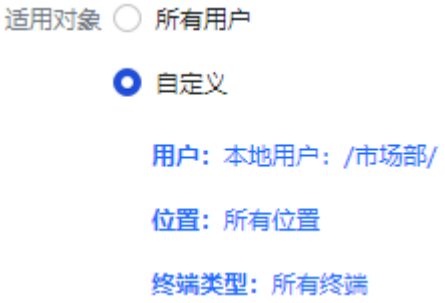
步骤1.自定义通道适用的应用。勾选[适用应用]栏右侧的[自定义]按钮。(勾选[所有应用]则表示该通道针对所有类型的数据都生效)。点击<请选择>按钮开始勾选特定的应用类型。

步骤2.在弹出框[自定义适用服务与应用]中选择应用：下载工具/全部，P2P/全部，P2P流媒体/全部。



步骤3.自定义通道适用对象。勾选[适用对象]栏右侧的[自定义]按钮(勾选[所有用户]则表示该通道针对所有用户均生效)。

步骤4.点击蓝色字体<用户>按钮，在弹出框[自定义适用对象]中选择指定对象。本次例中需要对市场部的所有用户做P2P流量限制，则此处选择“市场部”用户组，选择好[适用对象]后，点击<确定>完成设置。



步骤5.在[生效时间]栏内配置通道生效时间段，管理员可以视企业工作时间自定义生效时间段。

步骤6.在[生效时间]栏内点击<新增时间计划组>开始自定义策略生效时间段，点击<新增时间段>添加执行通道的时间。

步骤7.如果预设置通道生效日期，则点击[日期]栏后的配置按钮，添加计划时间段或者排除时间段。设置完成后点击<确认>按钮，最后点击<提交>。

步骤8.设置完成后，点击<确认>，完成保证通道的设置。点击<确定>保存后，看到提示信息后，点击<关闭>完成配置。

步骤9.配置完成，在流控策略列表查看到刚才配置的限制通道策略。

流量子通道

在某些场景下为了对已配置好的保证通道或者限制通道做更细腻化的带宽分配，需要借助流量子通道在一级通道的基础上再做二级流量管控。流量子通道与一级流量通道的对应关系如下所示：

1. 必须要有一级流量通道才能新建子通道。
2. 子通道的适用对象必须从属于一级流量通道的适用对象（适用对象包括用户组和用户）。
3. 子通道设置的应用服务必须从属于一级通道的应用服务。
4. 子通道设置的带宽值不能超过一级通道的最大带宽值。
5. 子通道对应的生效线路必须和一级通道一致。
6. 在配置流量子通道时，请注意上述对应关系否则会导致通道配置不生效。下文我们将通过示例来进一步展示如何配置流量子通道。

需求场景

公司租用了一条10Mbps电信线路，内网有1000名上网用户，保证所有用户的收发邮件流量在繁忙时也不小于3Mbps最大不能超过5Mbps，另外因为市场人员较多且收发邮件的应用比较重要，所以要在此保证带宽的基础上保证市场部人员的收发邮件流量在繁忙时也不小于1Mbps最大不能超过2Mbps，市场部同事限制单个用户的收发邮件流量占用带宽不超过160Kbps。

操作步骤

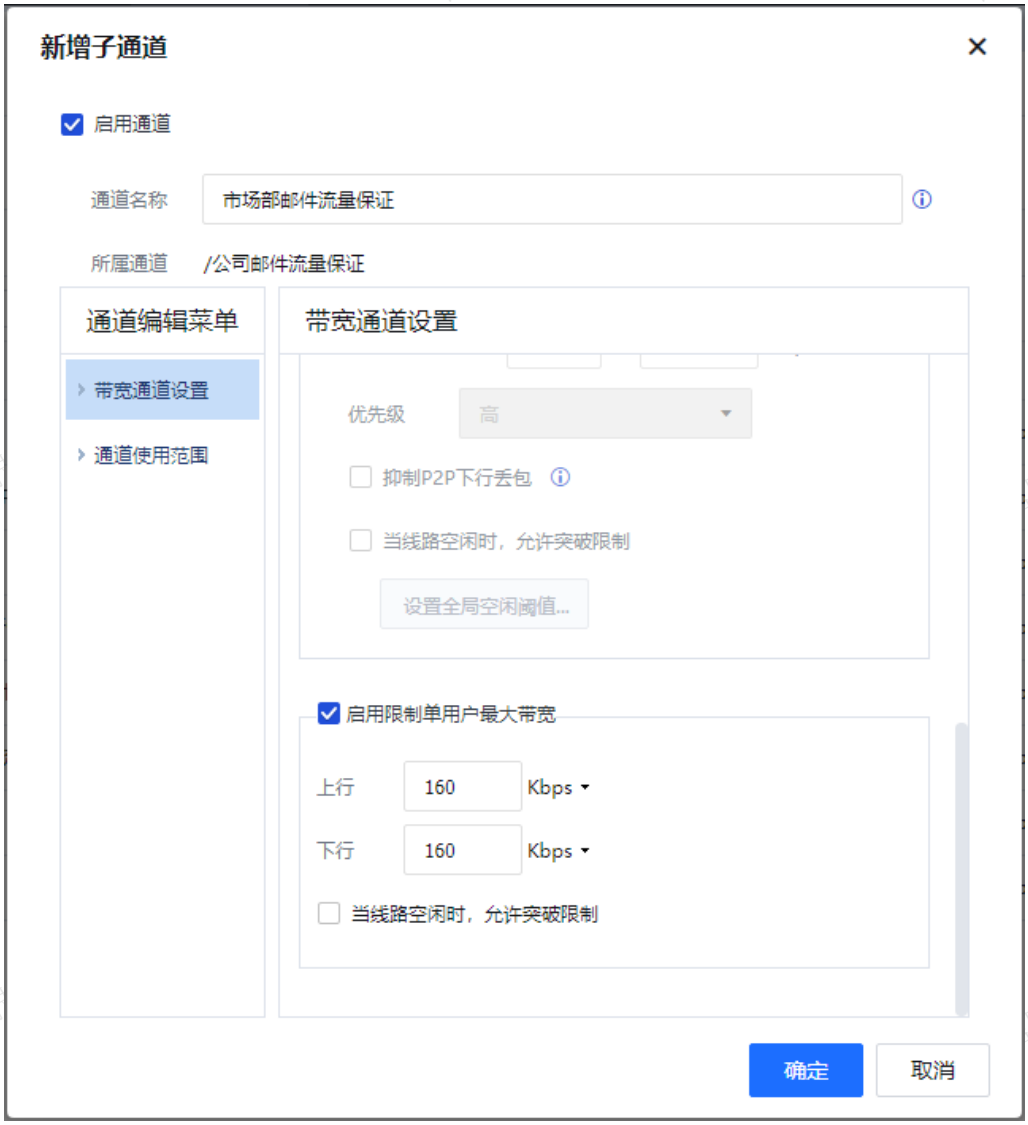
步骤1.建立保证公司所用用户邮件流量的一级流量通道。按照前文所示步骤先建立一级流量通道。此一级流量通道为保证通道，适用对象为所有用户，适用应用为邮件，对应的保证带宽为3Mbps，最大带宽为5Mbps。

步骤2.勾选文中所新建的流量一级通道后，在[流控策略/带宽分配/新增通道]中点击<新增子通道>。勾选[启用通道]然后在[通道名称]中输入该通道的名称。[所属通道]用于显示通道级别，此时通道级别应该显示为“/公司邮件流量保证”，表示该通道从属于“公司邮件流量保证”的一级通道。

步骤3.在[通道编辑]中选择[带宽通道设置]，在右边窗口中设置流量子通道的相关属性。

本次示例中需要保证市场部人员的收发邮件流量在繁忙时也不小于1Mbps最大不能超过2Mbps，市场部同事限制单个用户使用邮件应用占用带宽不超过160Kbps，所以此处勾选[保证通道]，设置[上行带宽]、[下行带

宽]的[保证]和[最大]分别为33%和40%的总带宽（此处的总带宽是父通道的保证和最大带宽值，非出口线路）。[优先级]勾选高。 勾选[启用限制单用户最大带宽]选项，将[上行]、[下行]的最大值都限制为160Kbps。



步骤4.在[通道使用范围]配置该子通道的生效范围，在右侧[通道使用范围]栏中设置通道适用的应用与对象用户。该子通道是为了保证市场部的邮件流量，因此适用对象需要自定义为市场部，适用应用会从属一级流量通道。

步骤5.设置完成后，点击确认，完成子通道的设置。在[带宽分配]中会显示设置好的一级通道和子通道。

步骤6.以模板策略新增子通道。在[流量控制/流量策略/带宽分配/新增通道]下提供以现有的流量通道为模板新增流量一级（子）通道的方式，目的是为减轻管理员配置工作。已经配置完成的流量通道会自动添加到模板中，管理员可以在模板中选择通道模板，进行简单修改，完成新流量通道的配置，如果是以某条子通道为模板新增流量子通道，则需要先勾选一级流量通道才能完成添加。

排除策略

排除策略用于设置某些类型的数据不匹配任何流量管理通道，设置排除策略的目的在于排除部分数据不经过流控。比如设备做网桥模式部署，前置防火墙的DMZ区接了部分服务器，内网访问这部分服务器的数据不需要经过公网，不需要受公网带宽的限制走流控通道，此时对这部分服务器的应用或者IP做排除策略。

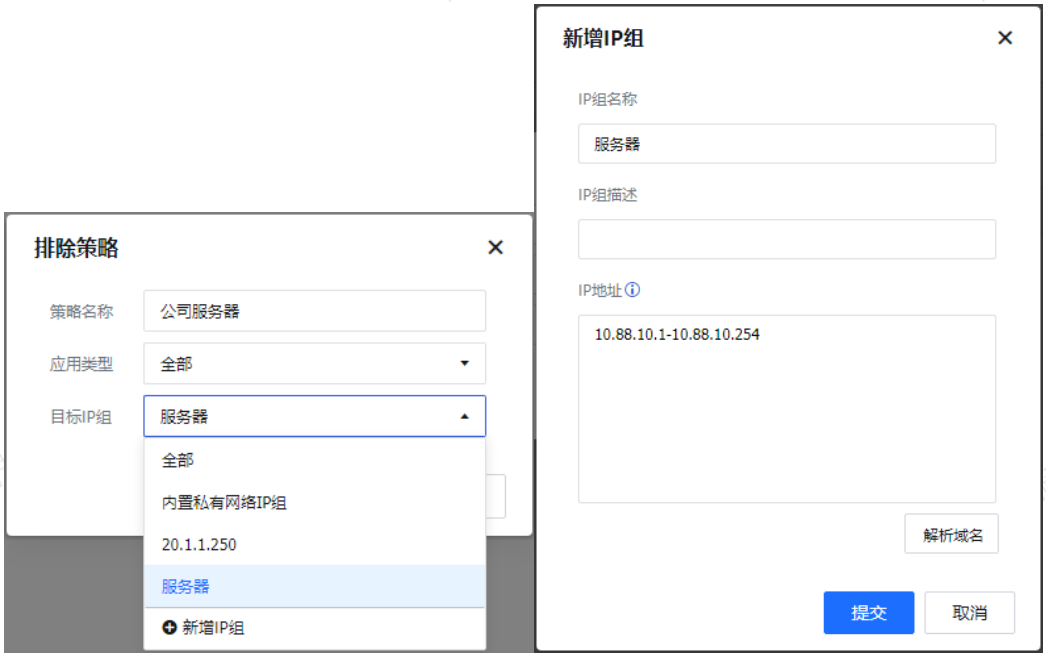
需求场景

设备做网桥模式部署，前置防火墙的DMZ区接了部分服务器，要对访问这些服务器的数据做排除。

操作步骤

步骤1.进入到[流控策略/排除策略]菜单栏，勾选[启用流量管理系统]。点击<新增>添加排除策略。

步骤2.在弹出的[排除策略]框中，输入排除策略名。[应用类型]栏按需勾选，默认为全选。在[目标IP组]展开下拉栏，点击<新增IP组>添加目标IP段。在弹出的[新增IP组]菜单的[IP组名称]栏中填写好IP组名称，在[IP地址]栏中填写好服务器IP地址段。



步骤3.最后点击<提交>按钮，排除策略成功配置后会显示在[排除策略]列表中。

惩罚通道

惩罚通道是一种特殊的流控限制通道。惩罚通道结合用户限额策略可在用户的流量在[使用总额]、[上线时长总额]、[网络流量速度]三种条件超出企业限制后匹配惩罚通道，对于匹配到惩罚通道的数据进行流量控制，控制占用的带宽不得超过惩罚通道设置的最大带宽值。惩罚通道的实现原理和限制通道相同，主要作用是结合[流量管理/用户限额策略]让超出限额的用户自动匹配到[流控通道/惩罚通道]，实现对用户的处罚。

需求场景

公司租用了一条20Mb/s电信线路，内网有1000名上网用户，发现很多市场部人员经常使用迅雷下载，P2P等下载工具进行下载，占用了大部分带宽，影响了其他部门的正常的办公业务。为了控制员工下载流量，限制市场部每用户每天下载流量不能超过1G，每月下载总流量不能超过30G。如有超出，则通过惩罚通道将超出限额的用户的带宽总和限制在520Kbps之内，并且每个超额用户占用的带宽限制在128Kbps，实现惩罚目的。

操作步骤

一、配置惩罚通道

本例中针对公司市场部人员在迅雷下载、P2P等下载流量超额后做惩罚。

步骤1.在[带宽分配]中点击<新增通道>，选择<新增惩罚通道>，在弹出的[新增惩罚通道]页面，勾选[启用通道]。在[通道名称]中输入该通道的名称，[所属通道]用于显示通道级别，“/”表示此通道是一级通道。

步骤2.在[新增惩罚通道]的[带宽通道设置]栏勾选[限制通道]，在[上行带宽]和[下行带宽]中设置最大为520Kbps。为了能够对每个超额用户的流量做限制，还需要勾选[启用限制单用户最大带宽]并在按照需求在[上行]、[下行]中填写最大带宽值为128Kbps。

二、通道生效范围

步骤1.在[通道使用范围]内配置惩罚通道的生效范围，在左侧[通道使用范围]栏中设置通道适用的应用与对象用户。此惩罚通道是针对下载总量超额后的市场部人员的所有流量做限制，因此适用应用是所有用户（超额后用户的总带宽最大为520Kbps，单用户最大128Kbps）。

步骤2.勾选[适用应用]栏右侧的<所有应用>。(勾选<所有应用>则表示该通道针对所有类型的数据都生效)。

步骤3.在[生效时间]栏可以设置此通道的生效时间，管理员可以视企业工作时间自定义生效时间段。

步骤4.在[生效时间]栏内点击<新增时间计划组>开始自定义策略生效时间段，点击<新增时间段>添加执行通道的时间。

步骤5.如果预设置通道生效日期，则点击[日期]栏后的配置按钮，添加计划时间段或者排除时间段。设置完成后点击<确认>按钮，最后点击<提交>。

步骤6.配置策略的[目标IP组]，可以结合前文[通道使用范围]里的[适用对象]来使用。在本次案例中：在[适用对象]里已设置通道对财务人员生效，因此在此处可以将[目标IP组]定义为全部。

步骤7.设置完成后，显示如下。

步骤8.设置完成后，点击<确认>，完成保证通道的设置。

到此，惩罚通道的相关配置已完成。适用对象以及超额的流量值需要在[流量管理/用户限额策略]里定义，通过[流量管理/用户限额策略]里的策略来调用该惩罚通道，实现对超额用户群的流量惩罚目的。在接下来的章节将详细介绍如何配置[用户限额策略]以及限额策略如何调用惩罚通道。

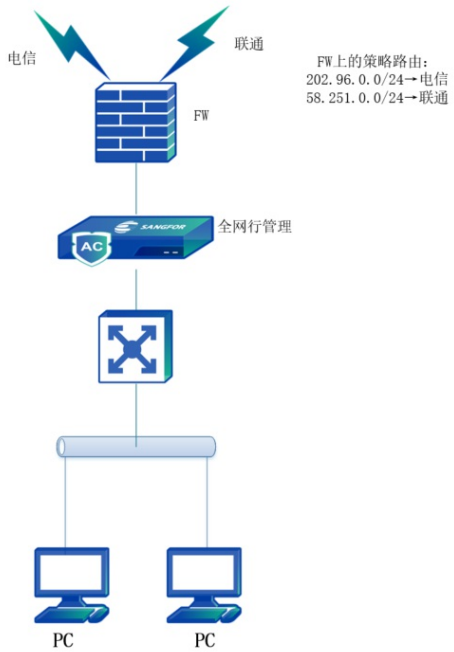
虚拟线路配置

设备在网桥模式下，无论前置设备上是接了多条线路还是单线路，或者设备以多网桥模式部署接了多个出口，对于AC设备而言经过设备的数据是一条线路的数据，设备流控策略默认是针对线路总和进行控制的，如果需要对多条线路区分控制，则需要借助虚拟线路的功能来实现。

默认情况下：即使AC设备的前置设备上有多条公网线路或者是AC设备以多网桥模式部署连接了多个出口，在虚拟线路配置中默认只有线路1，线路1的带宽设置应该设置成多条线路的总带宽，但此时设备无法对多条外网线路分别进行流控。

需求场景

设备以网桥模式部署，网络拓扑如下所示，防火墙上有两个出口，其中电信线路为10Mb/s，联通线路为10Mb/s，需求是对走两条线路的P2P数据分别进行流控，使P2P数据在两条线路上占用的带宽分别不超过20%。



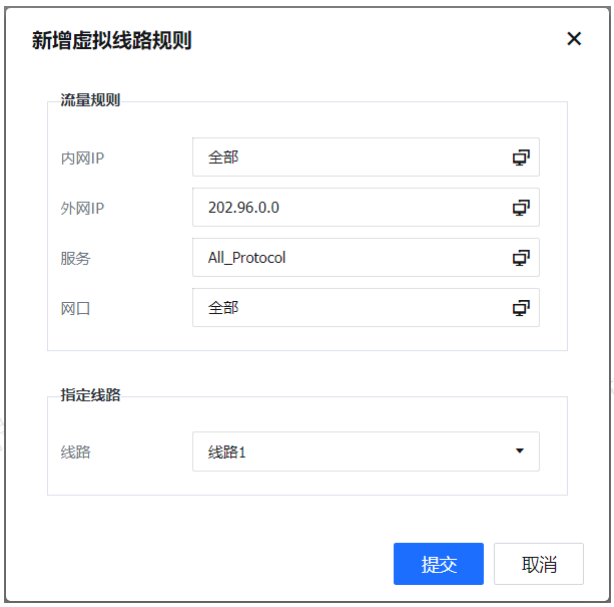
设置两条虚拟线路，分别对应FW上的两条公网线路，并且分别根据两条公网线路的实际带宽，设置虚拟线路的带宽。

操作步骤

步骤1.在[流量管理/虚拟线路配置/虚拟线路列表]中，点击<线路1>，编辑线路1的带宽值。在本次示例中，假设线路1为电信线路，则按照电信线路带宽配置如下参数。

步骤2.配置虚拟线路规则，新建的虚拟线路需要配置相应的虚拟线路规则才能生效，通过虚拟线路规则可以按照实际的选路规则将流量分配到不同的虚拟线路上，实现虚拟线路和实际线路的对应。

前置设备一般会有选路规则，按照前置设备上的选路规则配置虚拟线路规则即可。按照示图中的FW的规则：202.96.0.0/24电信。可为线路1配置如下规则。



- 内网IP：用于设置数据包的源IP，用户可以根据实际需求作对应的修改。
- 外网IP：用于设置数据包的目标IP，目标IP可以在[对象定义/IP地址库]中自定义。
- 服务：用于设置数据包所承载的服务。
- 网桥列表：用于在多网桥模式下，指定匹配该规则的数据是从哪个网桥所转发。本次案例中为单网桥模式，因选择全部网口。

• **指定线路：用于设置满足以上四个条件的数据走哪条目的虚拟线路。**

步骤3.根据前置FW上的选路规则，在AC设备上配置相对应的虚拟线路规则。

步骤4.配置流控策略分别管控两条虚拟线路上的P2P应用数据。在[流控管理/流控策略]里为线路1配置流量限制通道。

在[带宽分配]中点击<新增通道>，选择<新增一级通道>。[新增一级通道]菜单栏内设置好通道名、限制通道上下行带宽。在[通道使用范围/适用应用]里勾选P2P下载应用。（具体配置步骤请参考限制通道章节）

说明：

1．虚拟线路规则的匹配顺序是由上往下匹配，支持导入和导出。路由模式、网桥模式、单臂模式都支持配置虚拟线路规则。

2．路由模式支持选择物理选路模式和虚拟线路模式：

3．物理线路模式：真实的网络线路，于网络出口一一对应。

4．虚拟线路模式：可以将一条物理线路虚拟成多条线路或将多条物理线路虚拟成一条线路，针对虚拟出的线路进行流量管理。

DNS代理

深信服全网行为管理支持DNS代理。管理员可以根据不同域名配置不同的代理策略，同时可以结合终端用户群体、访问网站类型、访问域名、目标DNS地址等信息设置DNS代理策略的生效范围。

深信服全网行为管理设备可以提供如下DNS代理策略：

1. **重定向至DNS服务器**：DNS服务器的IP；
2. **解析为IP**：直接把域名解析为该IP；
3. **丢弃**：直接将DNS请求丢弃；
4. **重定向至指定线路**：重定向到指定的出口（运营商）。

重定向至DNS服务器

公司将全网行为管理设备以路由模式（网桥模式）部署在网络中，而内网用户A的电脑DNS地址被错误配置为3.3.3.3（无效DNS地址）。管理员希望将用户a访问www.baidu.com这个域名的请求，强制重定向至外网的114.114.114.114的DNS服务器，使得用户A的电脑即使配置的是无效DNS也能正常访问该域名。

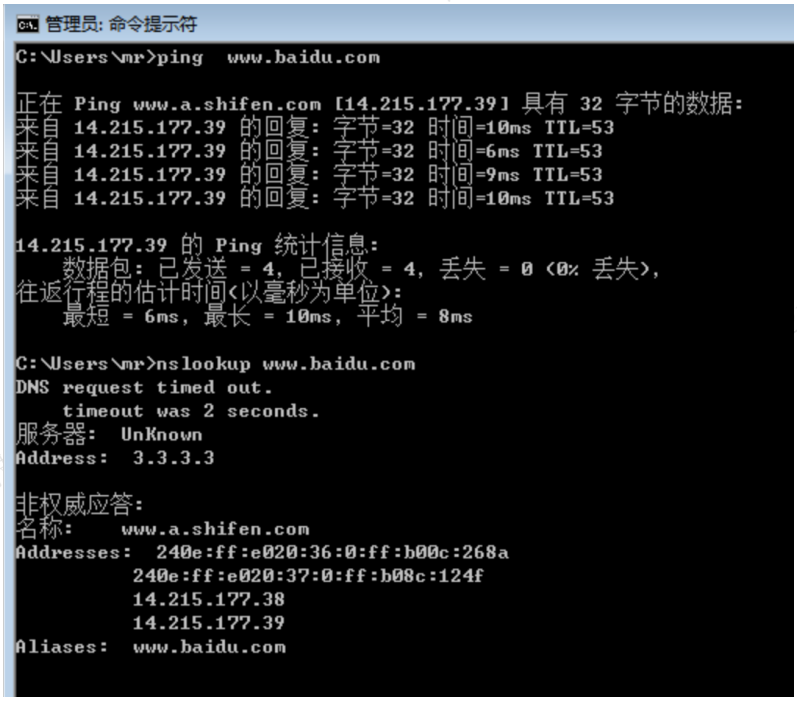
操作步骤

步骤1.配置代理条件，进入[流量管理/DNS代理]栏点击<新增>。在弹出的[编辑DNS代理/代理条件]页面中配置如下参数。

步骤2.将[用户]自定义为用户A,在[访问域名]自定义为www.baidu.com，在[目标DNS地址]栏自定地址为3.3.3.3。

步骤3.配置代理策略，在[代理策略]栏选择<重定向至DNS服务器>，然后在[DNS地址]配置期望的DNS地址114.114.114.114。

步骤4.验证代理策略是否生效。因为主机配置的无效DNS，导致无法正常访问www.baidu.com。但是因为AC的DNS代理的存在，用户A的电脑依旧能够正常访问www.baidu.com。



说明：

通过DNS代理将内网用户的DNS请求转发到内网DNS服务器（DNS服务器在DMZ区）时会出现如下现象：代理到内网DNS服务器失败（如果用户自己电脑有配置有效的DNS服务器，则走自己的DNS服务器，DNS服务器无效则会导致断网）。

解决办法：防火墙配置放通DMZ区->AC设备LAN口的流量。

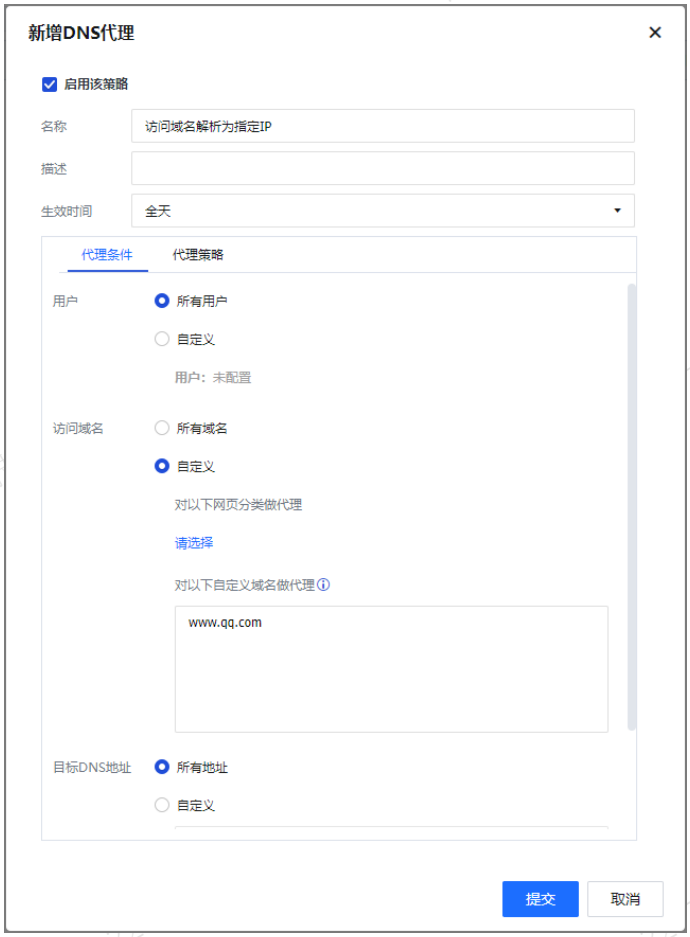
解析为指定IP

公司将全网行为管理设备以路由模式（网桥模式）部署，管理员希望将内网用户访问域名www.qq.com的请求强制解析为6.7.6.7。

操作步骤

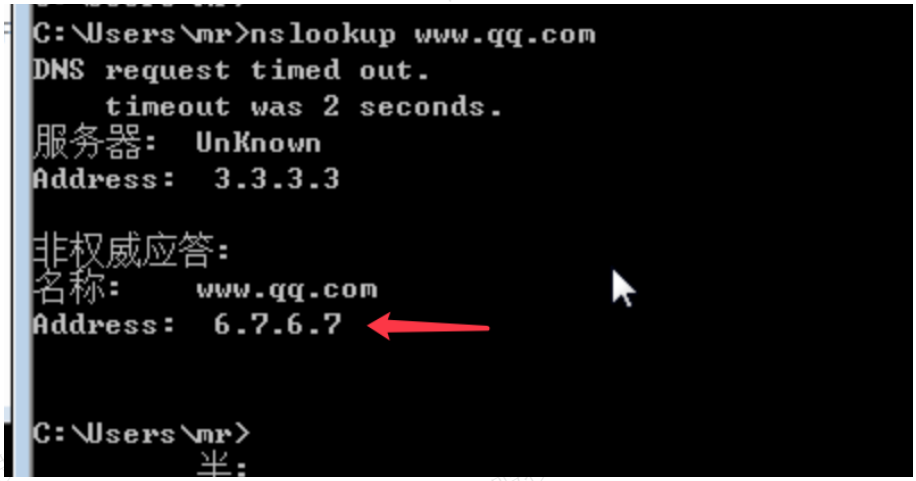
步骤1.配置代理条件，进入[流量管理/DNS代理]栏点击<新增>。在弹出的[编辑DNS代理/代理条件]页面。

步骤2.在[用户]栏将用户定义为所有用户，在[访问域名]栏自定义域名为 www.qq.com，在[目标DNS地址]栏内勾选所有地址。



步骤3.配置代理策略。在[编辑DNS代理/代理策略]栏选择“解析为IP”，然后在[IP地址]栏配置期望的IP地址。

步骤4.验证代理策略是否生效，在用户内网的测试PC上通过nslookup解析域名www.qq.com。



丢弃指定域名的访问

用户的AC设备以路由（网桥模式）部署，管理员期望内网用户访问域名www.sangfor.com.cn 时，AC设备能将这部分流量直接丢弃。

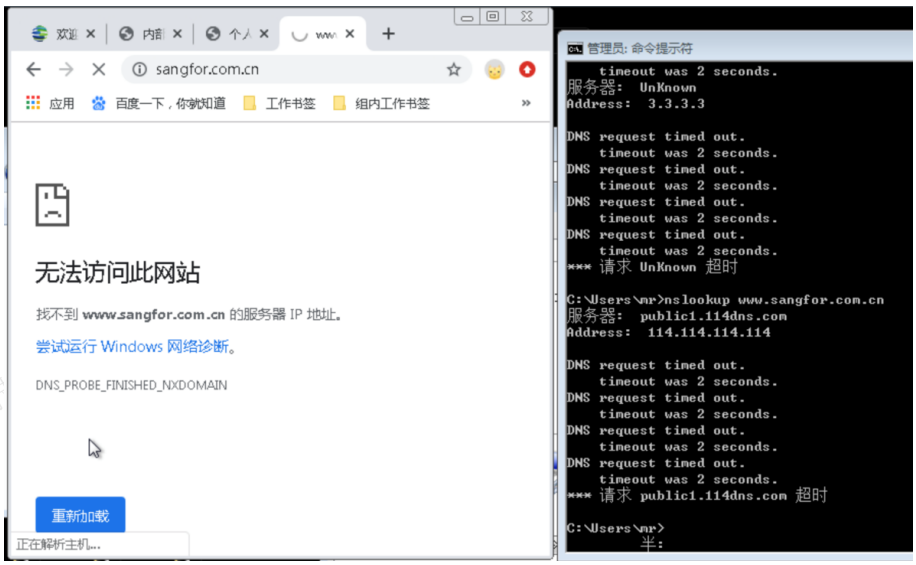
操作步骤

步骤1.配置代理条件，进入[流量管理/DNS代理]栏点击<新增>按钮配置，在弹出的[编辑DNS代理/代理条件]页面中配置如下参数。

步骤2.在[用户]栏将用户定义为所有用户，在[访问域名]栏自定义域名为www.sangfor.com.cn，在[目标DNS地址]栏内勾选所有地址。

步骤3.配置代理策略，在[编辑DNS代理/代理策略]中选择[丢弃]。

步骤4.验证代理策略是否生效，使用内网电脑通过nslookup解析www.sangfor.com.cn域名或者通过浏览器直接访问该域名。



重定向至指定线路

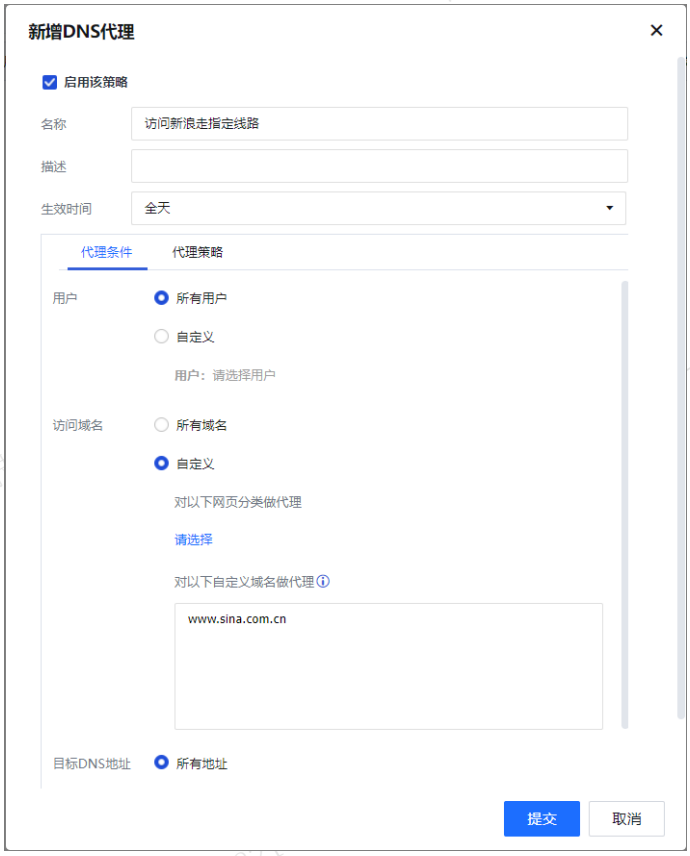
公司将全网行为管理设备以路由模式（网桥模式）部署在网络中，且开启了线路DNS和链路负载功能。管理员期望内网用户访问域名www.sina.com.cn的流量走线路2。

操作步骤

步骤1.配置DNS服务器和链路负载功能（开启链路负载功能请参考链路负载）。

步骤2.在[流量管理/虚拟线路配置/虚拟线路列表]内为各条线路配置DNS服务器。

步骤3.配置代理条件，进入[流量管理/DNS代理]栏点击<新增>配置，在弹出的[编辑DNS代理/代理条件]页面中将[用户]定义为所有用户，在[访问域名]栏自定义为www.sina.com.cn，在[目标DNS地址]栏的地址为所有地址。



步骤4.配置代理策略，在[编辑DNS代理/代理策略]栏选择[重定向至指定线路]。在[网口]勾选目标出口线路。只能选择设置了DNS和DSCP/TOS值的线路，未开启链路负载时，此功能不生效。

步骤5.验证代理策略是否生效使用测试电脑直接访问ww.sina.com.cn域名，在AC设备[流量状态/连接监控]里查看对该域名的访问流量是否是走线路2。

DNS代理逃生

DNS代理的[重定向至DNS服务器]和[重定向到指定线路]两个场景提供了逃生机制。当某条线路断了，DNS代理策略失效。

- 没有启用链路负载，直接走默认路由；
- 有启用链路负载，走负载策略；如果负载也异常了，走默认路由；

- **新增的默认路由页面，支持调整默认路由顺序；**
- **默认路由逃生机制，根据线路故障检测（DNS和ping）。**

注意事项

1. 当配置了将域名加入全局排除后，DNS代理[丢弃]策略不生效，开直通后DNS代理也不生效。
2. 网桥下DNS检测是从DMZ口发包出去检测，网桥部署场景需要保障DMZ口发包可以到达出口。
3. SG开启代理模式下不能做DNS代理。SG开启代理后DNS请求是由本机做了代理发起，DNS代理的功能无法对本机发包再做代理。
4. DNS代理策略只有在配置重定向至指定线路时才会和链路负载策略发生冲突。当两者配置冲突时，DNS代理策略优先级更高，以DNS代理策略配置的重定向线路为准。

链路负载

为了保障核心用户、核心应用上网体验，同时受限于有限的优质带宽资源，用户迫切希望能够把实时性和稳定性要求不高的应用（如：P2P、P2P流媒体、web流媒体、游戏等）引流到带宽大、质量一般的链路上去，将实时性和稳定性要求高的核心用户（如管理层等）和核心应用（如视频会议等）引流到优质线路上去，通过这种方式保障那些高实时性要求的应用体验，由此大大提高工作效率。

AC流量选路支持通过IP，协议、用户选路、应用选路、网桥场景选路、DNS代理等流量优化功能，提升用户带宽利用率。

引流方案说明

引流方案支持多种部署方式，以路由模式部署实现应用引流。也能够和主流厂家的路由器/防火墙结合，支持基于标签的引流，满足用户不同链路接入的场景。

深信服全网行为管理采用应用路由技术、DNS透明代理技术以及链路繁忙控制等技术实现基于链路的负荷情况、时间段、用户群体、访问对象等因素分将流量分配链路的分配机制，进一步提升链路优化使用率。

深信服全网行为管理支持按照终端用户群体、上网应用、访问域名、源地址段、目的地址段、传输协议、IP层DSCP/TOS标记等因素来设置引流范围，支持动态负载（优先使用高优先级线路）、指定线路、按运营商负载、按线路带宽负载、按剩余带宽负载、VPN做专线备份等多种负载方式，提升引流效果。

[应用路由技术]

深信服全网行为管理采用应用路由技术实现基于链路的负荷情况、时间段、用户群体、访问对象、访问应用类型等因素来分配链路的分配机制，进一步提升链路优化使用率。

[动态引流技术]

深信服全网行为管理采用动态引流技术，优质线路空闲时其他用户和流量也可以跑优质线路，优质线路快要繁忙时，引走非核心应用流量和非核心用户流量，在保障核心用户和核心应用的上网体验前提下，对优质线路充分利用，避免空置浪费。

[选路支持说明]

路由模式和网桥模式支持链路负载。支持DSCP和tos标记。

默认负载策略优先级：禁用默认负载策略、优先使用优先级最高的线路、按运营商负载、剩余带宽、带宽比例、平均分配。

优先负载策略：指定线路、多线路负载、剩余带宽、优先使用前面线路、带宽比例、平均分配、VPN做专线备份。

网桥模式选路

高校场景使用此场景更多。单位出口多条线路，部署了AD设备，AC网桥模式串接部署，期望实现和出口设备联动实现选路。“核心应用”走线路一，游戏等非工作应用走线路二。

前置条件：

1. AC配置链路负载，指定线路AD和AC设备同时用tos标签标识线路。
2. AC设备网桥模式部署，有两条外网线路，线路一是电信线路800M，线路二是联通线路500M。
3. AC最少有两条外网线路，可在[系统管理/系统配置/授权管理]页面查看设备的线路情况。

操作步骤

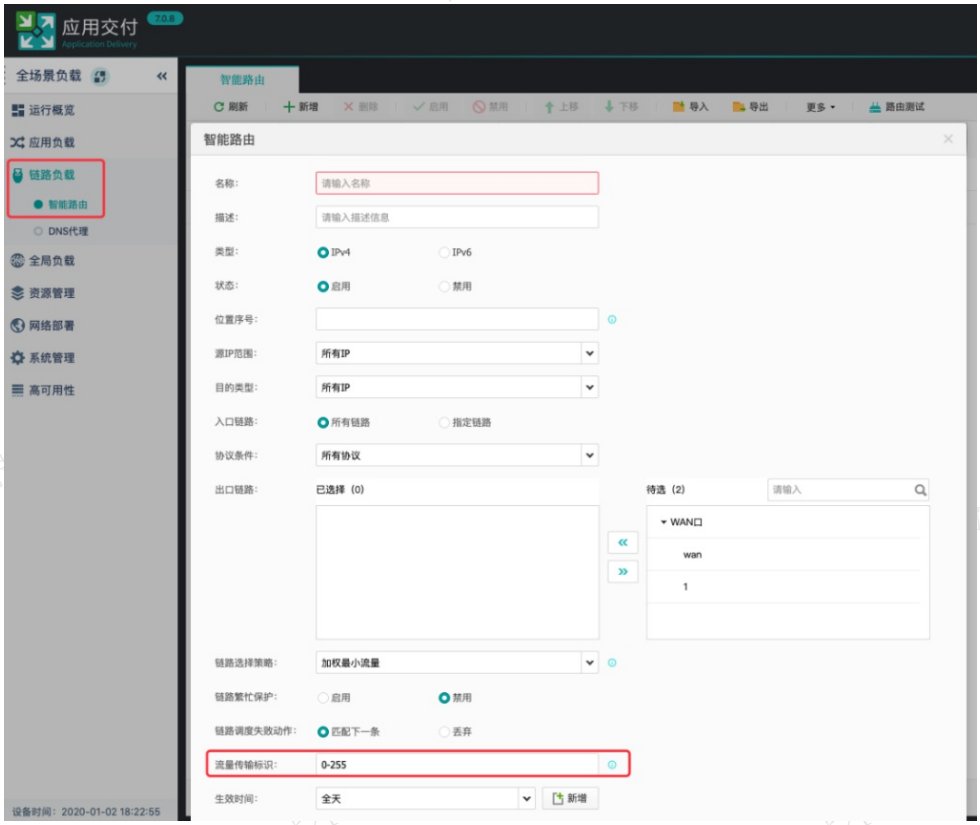
步骤1.部署模式配置。在[系统管理/网络配置/部署模式]栏将部署模式配置为网桥模式，并且配置好DNS地址。

步骤2.定义虚拟线路。在[流量管理/虚拟线路配置]，定义虚拟线路的tos值，tos值需要与出口AD上的值保持一致。

虚拟线路列表 虚拟线路规则

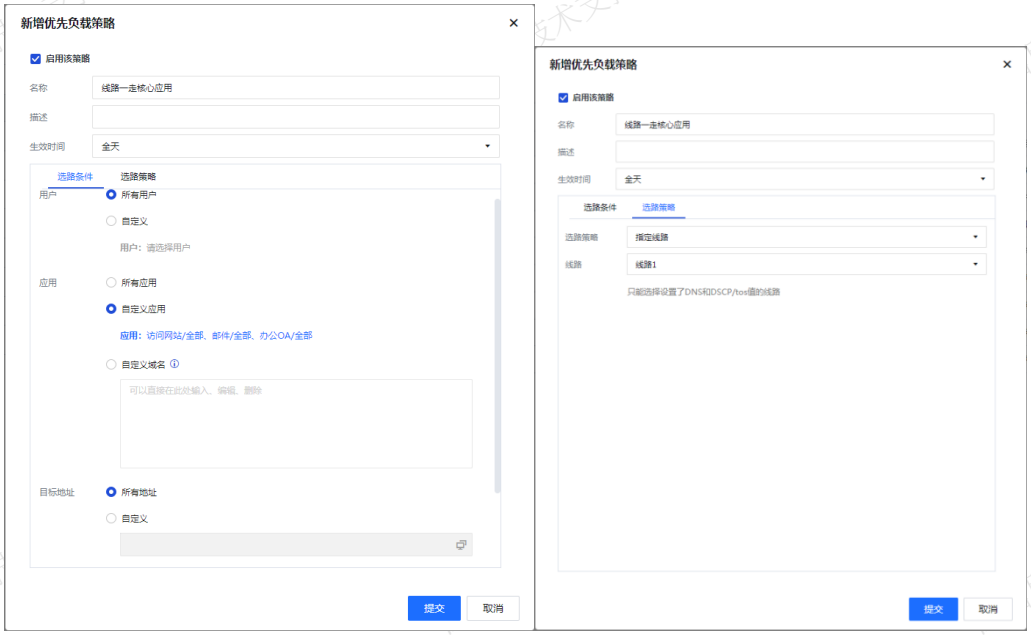
新增 高级设置

序号	线路	上行	下行	操作
1	线路1	800(Mbps)	800(Mbps)	删除
2	线路2	500(Mbps)	500(Mbps)	删除

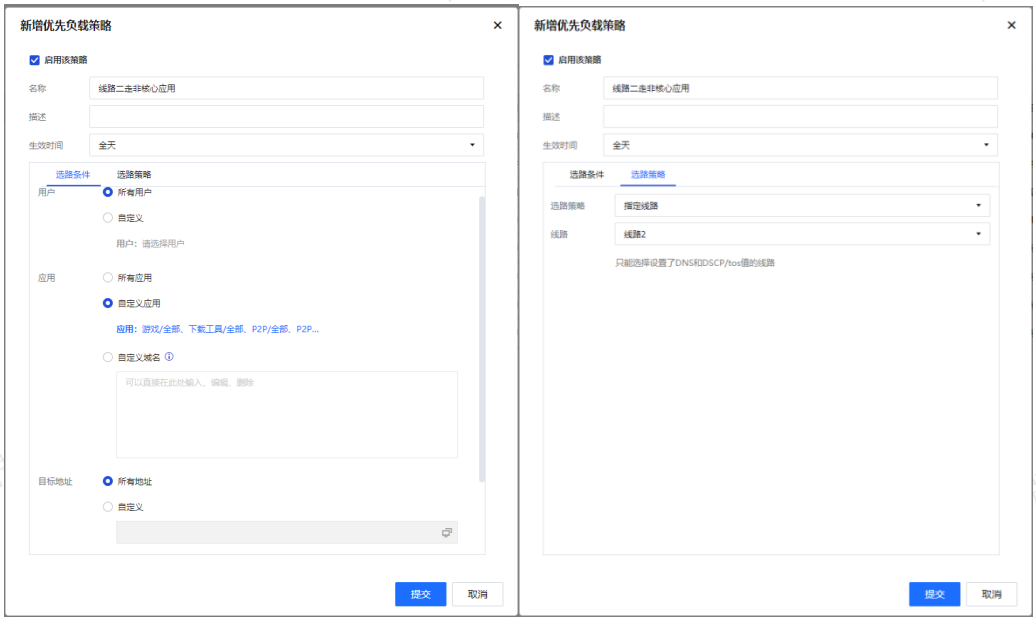


步骤3.配置链路负载均衡策略。在[流量管理/链路负载]勾选[启用负载均衡]，配置负载均衡策略。

线路1走企业核心应用。



线路2走企业非核心应用。

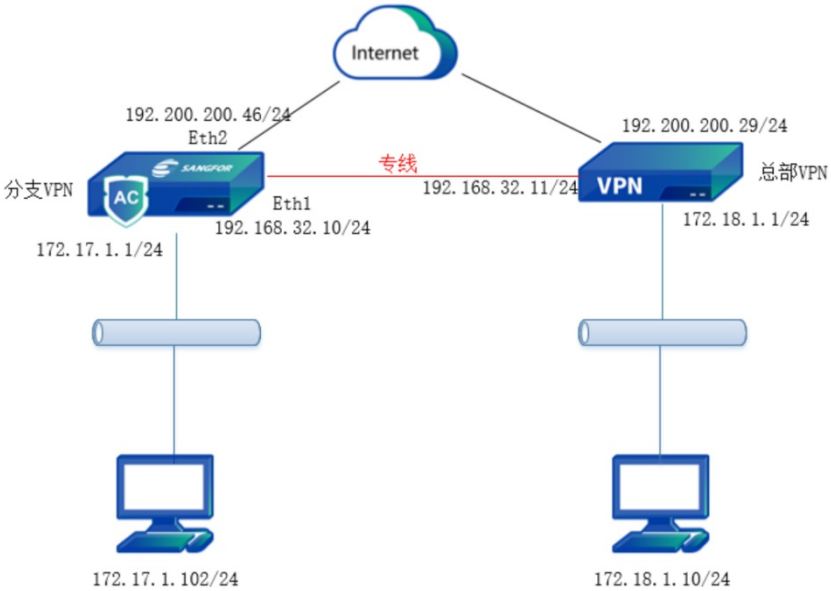


步骤4.确认配置结果。

路由模式选路

用户分公司在地市出口使用AC，分公司内网员工有访问省公司内网应用的需求，分公司AC和总部省公司出口设备连接了VPN，同时分公司和省公司连接了专线，现希望专线正常时分公司访问省公司应用走专线，当专线断开的时候，分公司访问总公司应用自动切换到VPN线路。

设备路由模式部署，有两条外网线路一条外网线路用于连接VPN，另外一条专线连接总部。



前置条件

1. AC最少有两条外网线路，一条用于连接VPN，一条用于连接专线。
2. 分支内网的网段，以及需要访问的总部内网网段要了解，清楚分支和总部的整体部署，总部哪台设备用来提供VPN对接，专线连接总部哪台设备哪个网口。
3. 确认总部VPN设备是我们公司自己的VPN设备还是第三方VPN设备，如果是我们自己的VPN设备总部要事先创建好VPN账号供分支VPN连接；如果总部是第三方VPN要知道第三方VPN第一阶段第二阶段对接的相关参数。

预期效果

专线和VPN连接正常时，分支访问总部应用优先走专线，专线断切换走VPN线路。

操作步骤

步骤1.将部署模式配置为路由模式，并且配置好内外网口，以及两条外网线路的地址。

步骤2.静态路由配置。如果分支内网是三层环境，还需要添加内网的回包路由网关指向内网的三层交换机。此环境中内网是二层环境无需添加静态路由。

步骤3.配置VPN连接管理连接总部VPN设备。

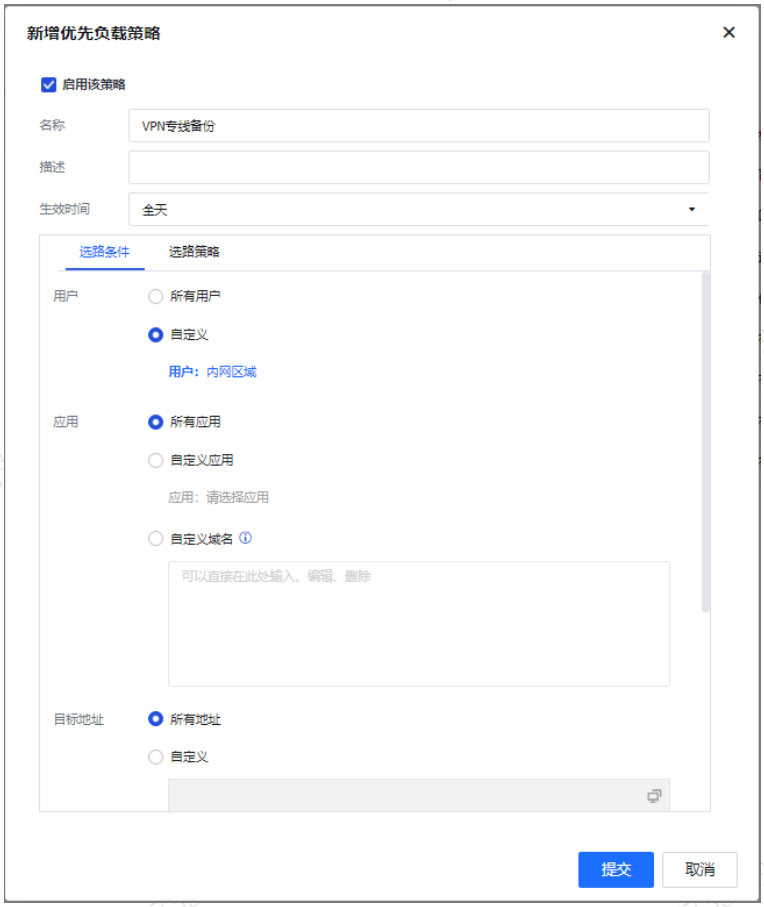
步骤4.配置完成VPN连接成功可以看到VPN连接成功，总部内网网段的路由指向VPNTUN口。

说明：

如果总部VPN设备是第三方VPN产品，非我们自己公司的VPN设备同样是支持的，但是此时配置VPN时要配置第三方VPN对接，并且总部VPN设备或者总部网络要支持分支内网访问总部应用走专线时，总部要从专线回包到分支内网；分支内网访问总部应用走VPN时，总部要从VPN回包到分支内网。

步骤5.配置链路负载，在[对象定义/IP组/IP组列表]栏中定义分支AC内网的IP范围段以及总部的范围段。

步骤6.在[流量管理/链路负载]新增VPN专线备份的多线路负载均衡路由。



步骤7.配置两条外网线路的线路故障检测。

说明：

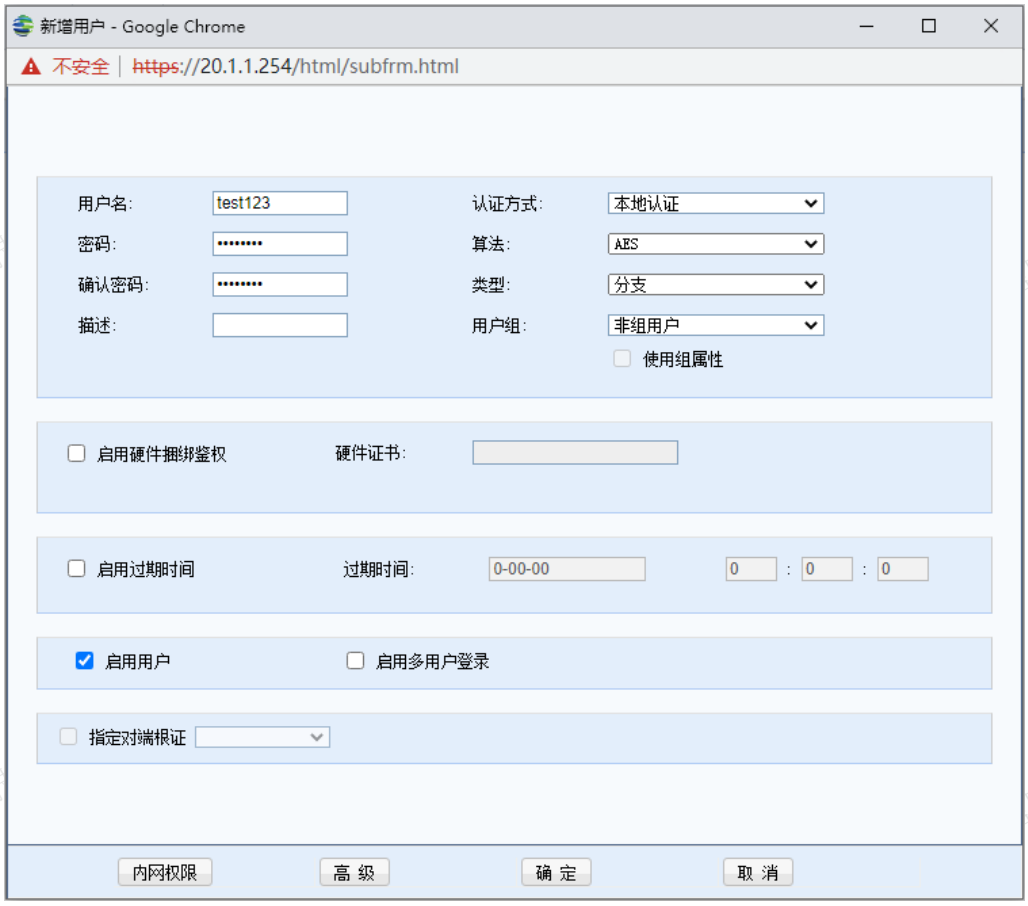
线路故障检测，有DNS解析和ping两种链路状态监测方法，可以自行选择：

1. Ping和DNS检测任意一个不通了，则认为不通了。
2. Ping和DNS里可以填多个地址；多个地址之间是或的关系有一个成功即成功。
3. 自动检测，表示是否开启了自动检测。如果不开启自动检测，那么只要网口有电，就认为网络是通的。

步骤8.配置总部VPN。总部VPN设备一般事先已经上架好了、部署设置和路由都是配置好的这里以AC的设备来截图配置。

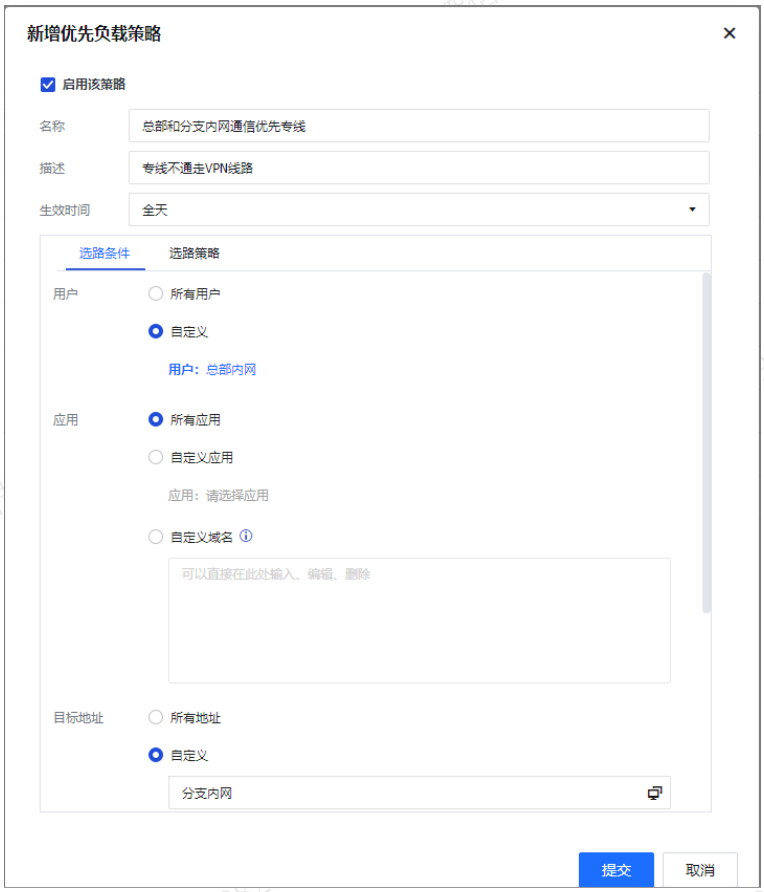
步骤9.检查部署模式，部署模式配置网关模式，有两条外网线路。线路2是专线，连接分支AC。

步骤10.由于此处AC为内网二层环境，没有配置静态路由。配置总部VPN服务端监听的地址和端口并创建账号。



步骤11.在总部AC的[系统管理/对象定义/IP地址库/IP组]定义总部内网IP地址端以及分支的IP地址段。

步骤12.在[流量管理/链路负载/优先负载策略]中配置优先负载策略。



说明

：

1. 总部设备可以是深信服VPN设备也可以是第三方VPN设备，分支专线连接总部可以连接总部VPN设备也可以连接到总部内网其它设备，但是总部要保证，分支内网访问总部应用的数据走专线时总部的回包也从专

线回包，分支内网访问总部应用的数据走VPN时总部也会从VPN回包。总部要配置好相关的策略路由或者选路规则。

2. 总部配置好选路策略后也可以实现，总部访问分支内网优先走专线，专线断开走VPN线路。

步骤13.验证选路效果。

AC内网测试总部内网的应用正常走专线，查看AC VPN确认有没有流量，正常情况下是没有流量的。

拔掉ETH1口的专线，此使数据切换至VPN线路。再次查看VPN链路上是否有数据。

说明：

尽量选择不同的应用做拔线切换的测试，如专线正常前测试的是http://172.18.1.10，那么专线断开后可以测试其他服务器的应用。如果拔线切换前后测试的是同一应用那么断开当前应用重新测试。

指定线路选路

用户AC有两条外网线路一条联通一条电信，现在想实现内网访问电信的数据走电信的线路，访问联通的数据走联通线路。

解决方案：链路负载策略，内网的源地址，设置指定的目标地址选择走相应的线路。

多线路负载

深信服全网行为管理为用户提供多种线路负载方案，本节内容主要阐述各个方案的具体应用场景以及配置方法。

一、优先使用优先级最高的线路

当用户出口拥有多条出口链路时，在深信服全网行为管理设备上可以呈现出每条线路的状态。管理员可以根据线路的状态定义优先级。当线路出现繁忙状态时，为了保证企业核心用户和核心业务的流量，可以选择让这部分核心流量走优先级最高的线路，把非核心流量引走到其他链路。

进入[流量管理/链路负载]，在[默认负载策略]栏勾选<优先使用优先级最高的线路>，[优先保证的用户]栏定义核心用户，在[线路繁忙时引走的应用]栏定义好线路繁忙时需要引走的应用流量。最后再定义好各线路的优先级。

二、按运营商负载

当用户出口拥有不同运营商的出口链路，管理员可以根据目的地址所在运营商将流量负载到对应运营商的线路商，前提是需要管理员定义好每条链路的DNS。DNS请求的流量支持选择独立负载方式。

进入[流量管理/链路负载]，在[默认负载策略]栏勾选<按运营商负载>。在[线路信息]栏定义好各个线路的DNS信息。对DNS请求的流量如果需要做其他特殊负载的话，可以勾选[将DNS请求负载到多条线路]，负载方式可以独立于运营商负载策略。

三、平均分配

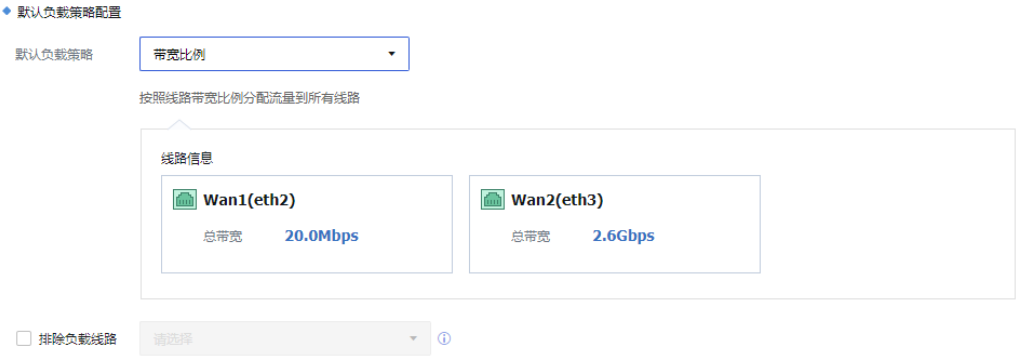
当用户出口拥有多条出口链路时，管理员可以选择将流量平均分配到各条线路上。

进入[流量管理/链路负载]，在[默认负载策略]栏勾选“按运营商负载”。

四、带宽比例负载

当用户出口拥有多条出口链路，但各条链路的带宽大小不一致。管理员可以根据各链路不同的带宽值赋予权值，深信服全网行为管理设备时将按照链路的权值分配流量，权值越大选择的机会越大。

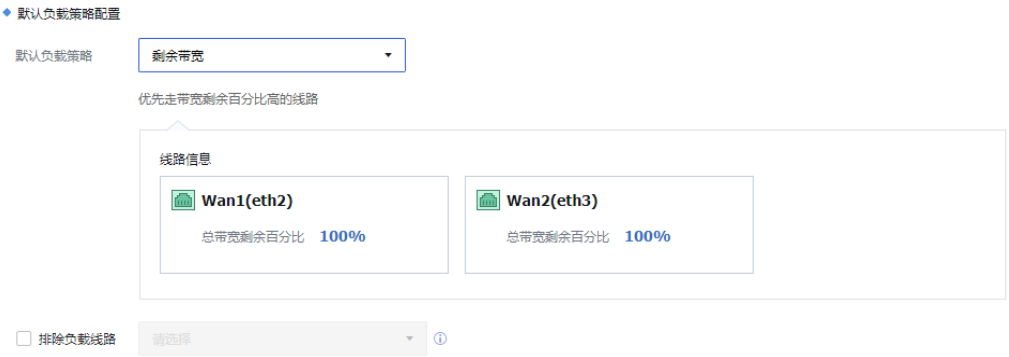
在[流量管理/链路负载]，在[默认负载策略]栏勾选“带宽比例”。在[线路信息]栏定义每条出口链路的总带宽值。



五、剩余带宽

当用户出口拥有多条出口链路，各条链路的利用率不同时。管理员可以根据各链路当前剩余的带宽百分比分配流量。

进入[流量管理/链路负载]，在[默认负载策略]栏勾选<剩余带宽>。在[线路信息]栏会展现当前各条线总带宽剩余百分比，开启<剩余带宽>负载策略后，流量会优先走带宽剩余最多的链路。



流量可视化

在[流控策略]可以通过点击<线路>进入线路可视化状态，查看当前使用情况。

点击[通道实时信息]栏内右侧的<查看>按钮，查看通道当前的使用情况。

注意事项

1. SG开启代理模式下不支持运营商负载按DNS负载选线路。运营商按DNS负载选路实际上就是需要对DNS做代理，SG开启代理后DNS请求都由本机代理发起，无法重新再驱动代理。
2. SG开启代理模式下，不支持应用选路。
3. 主主模式不会同步网络相关配置。链路负载和DSCP这些都是属于网络配置。只会在单个节点生效。
4. 开全局排除、直通，链路负载功能不丢包，功能依然生效的。
5. 链路负载功能不支持告警。
6. SG开启显示代理或开启SSL解密的情况下，不支持链路负载。
7. 应用选路场景：部分应用做了识别细分，每一个细分应用认为是一个应用，一类应用建议全部勾选，否则会影响选路效果。

路由模式的优先级说明：

1. 直连路由>静态路由>动态路由>DNS代理[重定向至指定线路]>优先负载策略>默认负载策略>默认路由。（没有配置VPN、没有专线备份场景）
2. 直连路由>静态路由>动态路由>DNS代理[重定向至指定线路]>优先负载策略>默认负载策略>默认路由>系统默认路由。
3. VPN路由>直连路由>静态路由>动态路由>DNS代理[重定向至指定线路]>优先负载策略>默认负载策略>默认路由>系统默认路由。

网桥模式的优先级说明：

4. DNS代理[重定向至指定线路]>优先负载策略>默认负载策略。
5. 当用户的流量出口场景为内网-AC（网桥）-代理服务器-F5时，不支持链路负载功能。
6. 配置链路负载，只要有多条外网线路，都需要配置<链路故障检测>功能。否则，链路负载策略配置后不生效。

用户限额策略

用户限制策略可以限制用户能使用的网络资源的流量和时长，包括流量配额，上网时长控制和并发连接数控

制，以及在线终端数量限制。接前文惩罚通道的示例我们继续来配置用户限额策略，通过本次配置的用户限额策略来调用前文所配置的惩罚通道。

流量配额

在前文中我们已经按照需求将惩罚通道配置完成。接下来只需配置流量限额策略并在策略里调用流量惩罚通道即可。

需求场景

某企业要求市场部每天的迅雷下载、P2P下载量不能超过1G，每个月的下载总量不能超过30G，因此按照要求配置流量限额策略。

操作步骤

步骤1.点击[流量管理/用户限额策略]的<新增>，点击<用户限额策略>。在弹出的[用户限额策略]菜单栏中勾选<启用该策略>，填写策略名称、描述信息。

步骤2. 在[用户限额策略]栏中勾选[流量配额]，在[流量配额]栏中配置流量配额参数。

本次示例中是针对市场部人员迅雷下载、P2P下载量进行限额配置，限额量为每天最多1G，每月最多30G。因此在[单用户流量限额配置]栏里的[统计时间]栏中勾选为全天，也可以自定时间段，与前文流量通道里的自定义时间段配置方法一致。点击<统计应用>，在弹出的[选择适用应用]中勾选全部的P2P应用。日配额按照需求填写1GB，月配额填写30GB。

步骤3.在[限额超出处理]栏中可以对超出时长配额的用户配置如下三种处罚措施。

• 选择发送告警邮件通知管理员用户已经超额信息（此功能需要AC与企业的邮箱系统完成对接，才能正常发送告警邮件）。

• 选择提醒即将超额或者超额的用户，告知用户他的时长配额即将超额。

• 选择将超额用户添加到处罚通道中或者是禁止超额用户上网。如果需要通过惩罚通道来对超额用户做惩罚，则需要在[流控策略]里提前配置好惩罚通道，然后在[限额超出处理]页面勾选[添加到流控通道]，然后选择对应的惩罚通道对超额用户做惩罚措施。

步骤1.在[用户限额策略]栏内点击[适用对象]选择限额策略生效对象。本次示例中是为了限制市场部人员P2P的下载量，因此在适用对象里勾选市场部人员即可。

步骤2.在[用户限额策略]栏内点击[高级配置]菜单栏。高级配置中包含[策略过期日期设置]、[同级别管理员查看编辑权限设置]、[允许低级管理员查看]。

步骤3.配置完成，在用户限额列表会显示刚配置的限额策略。

时长配额

时长配额用于限制单个用户在策略生效时间段内的上网时长，当某用户在策略生效时间段内应用时长或在线时长超过了限制值时，会禁止该用户上网或调用惩罚通道进行相应的惩罚。时长类型有应用时长配额和在线时长配额两种，用户可以根据需求选择对应的配额类型。

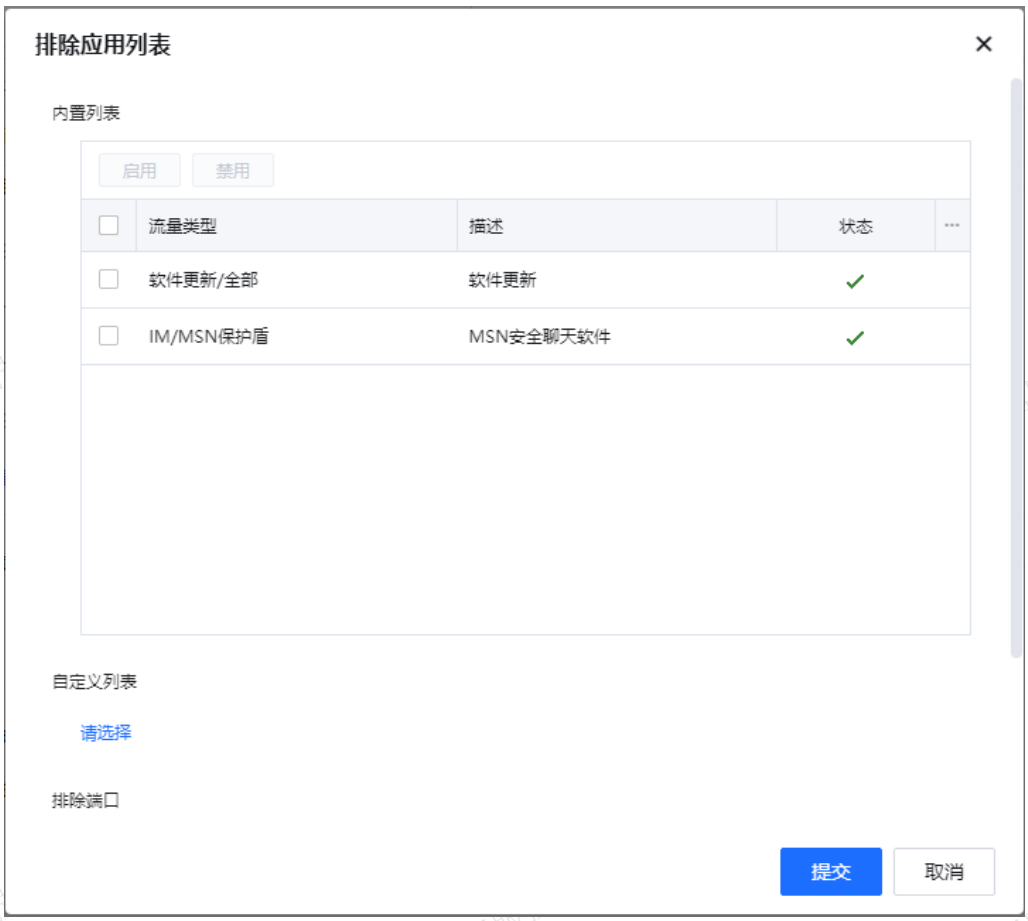
应用时长配额

步骤1.在[时长配额]界面的[单用户每天时长限额配置]栏内勾选[应用时长]。在[统计时间]栏内可以根据企业需求自定义配额时间段。

步骤2.在[统计应用]栏内可以根据企业需求勾选需要配额的应用，也可以勾选全部应用然后在<设置排除应用列表>设置白名单应用。

步骤3.点击<设置排除应用列表>。

步骤4.在弹出的[排除应用列表]页面中点击[自定义列表]栏下的<请选择>，在弹出的界面中勾选需要排除的应用或在[排除端口]中填写对应应用的端口即可。



步骤5.在[时长配额]栏里可以配置单用户的上网时长配置，单位为分钟，最大设置1440分钟(24小时)。

在线时长配额

在时长配额界面的[单用户每天时长限额配置]栏内勾选[在线时长]。在[时长配额]栏内可以根据需求定义单用户每天的上线时长。同时也可以设置排除应用，用户使用加入排除栏的应用时不会计算在时长内。

在[限额超出处理]栏中可以对超出时长配额的用户配置如下三种处罚措施。

• 选择发送告警邮件通知管理员用户已经超额信息（此功能需要AC与企业的邮箱系统完成对接，才能正常发送告警邮件）。

• 选择提醒即将超额或者超额的用户，告知用户他的时长配额即将超额。

• 选择将超额用户添加到处罚通道中或者是禁止超额用户上网。如果需要通过惩罚通道来对超额用户做惩罚，则需要在[流控策略]里提前配置好惩罚通道，然后在[限额超出处理]页面勾选[添加到流控通道]，然后选择对应的惩罚通道对超额用户做惩罚措施。

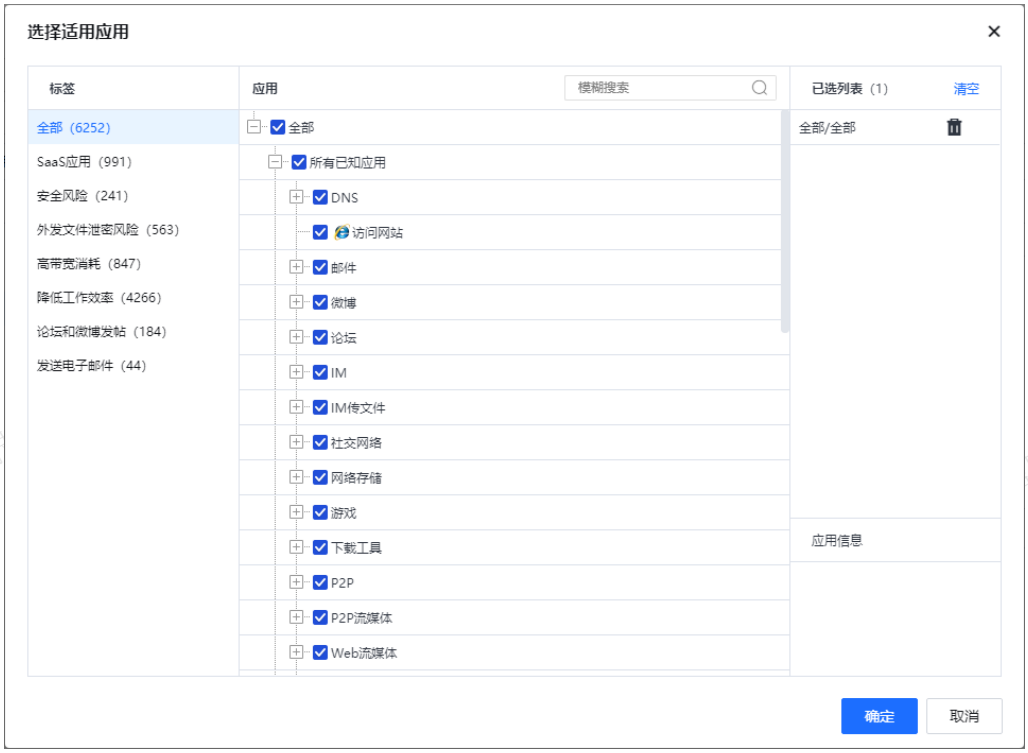
流速限制

流速限制用于检测单个用户在策略生效时间段内的流速情况，当用户在策略生效时间段内全部应用（特定应用）的总流量（上行流量或下行流量）持续超过设定的流量阈值多少分钟，将禁止此用户上网或调用惩罚通道进行相应的惩罚。

操作步骤

步骤1.在[流速限制]界面的[单用户实时流量长限额配置]栏内的[统计时间]栏，根据企业需求自定义限制时间段。

步骤2.在[统计应用]栏根据需求勾选特定的应用或者是全部的应用。



步骤3.在[流量类型]栏内可以选择策略检测的流量类型，可以选择上行流量、下行流量或者是总流量的流速。

步骤4.在[流速阈值]栏填写策略检测的流速阈值，在[超出阈值持续时间]栏里按照需求填写时间。比如企业

要对总流量持续30分钟超过2Mbps的用户做限制，则在[流量阈值]栏填写2Mbps，在[超出阈值持续时间]填写30分钟。

并发连接数控制

[并发连接数控制]用于限制单个用户的最大并发连接数。可以限制用户使用扫描工具或者P2P下载工具等同时开启大量连接的工具。也可以降低病毒通过内网扫描大量连接其他机器来传播病毒的机率。

在[并发连接数限制]选项中，能够填写的最大值为65535。

当用户当前建立的连接数超过[并发连接数限制]里连接数值时，可以通过邮件通知管理员，同时可以选择禁止用户创建新的连接或者指定用户多少分钟内禁止上网。

在线终端限制

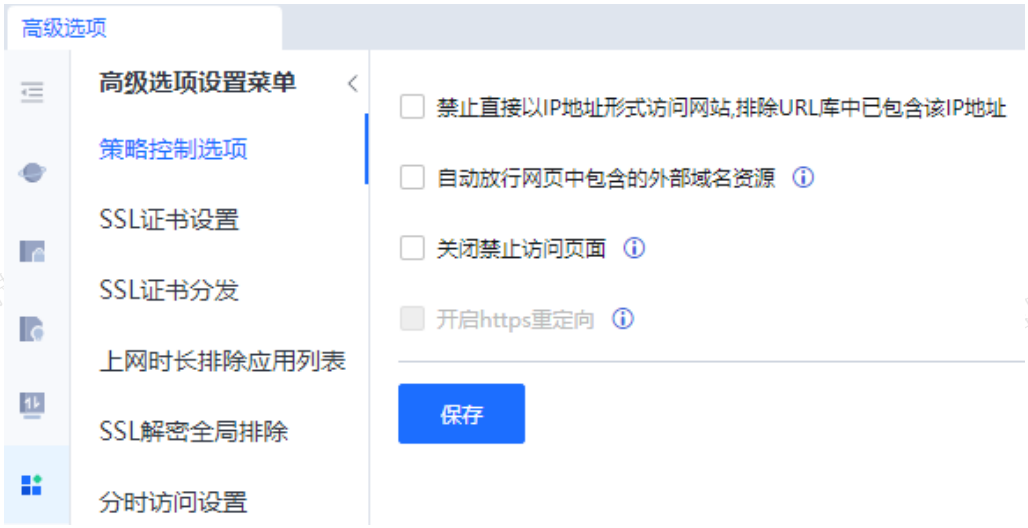
[在线终端限制]用于限制单个用户同时在线的终端数。可以结合策略[适用对象]对不同的用户做不同的终端限额策略，实现不同用户允许同时在线不同的终端数。

高级选项

高级选项设置包括策略控制选项、SSL证书设置、SSL证书分发、上网时长排除应用列表、SSL解决全局排除、分时访问设置。

策略控制选项

策略控制选项用于设置设备在进行URL过滤权限控制策略的匹配时，是否禁止直接以IP地址访问网站排除URL库中已包括该IP地址，是否自动放行网页中包含的外部域名资源和是否关闭禁止访问页面，是否开启https重定向功能，点击<提交>后才能生效。



禁止直接以IP地址形式访问网站，除非URL库中已包含该IP地址：勾选此选项后将禁止内网用户通过IP地址的形式去访问网站，如果该IP地址已经在URL库中被收录了，则不受此勾选的限制。

自动放行网页中包含的外部域名资源：用户访问网页的时候，这些页面中包含的外部域名资源（如广告、外部图片等）可能因为URL类型与主域名不一致，被策略拒绝，导致页面显示不完整。在这种情况下，勾选此选项可以在页面的主域名允许被访问的前提下，自动放行此页面中包含的外部域名资源，保证页面显示的完整性。

关闭禁止访问页面：如果关闭禁止访问页面，用户访问被禁止的网站或发表带有关键字的内容将不会显示禁止访问重定向页面。

开启HTTPS重定向：勾选开启HTTPS重定向功能，HTTPS流量被[访问权限策略/应用控制]拒绝时，能够显示重定向页面。

SSL证书设置

当设备开启SSL内容识别功能，终端浏览器会警告HTTPS网站证书无法验证，在终端电脑上导入证书可以解除告警。设备不仅支持导入深信服设备内置的根证书还支持自定义证书导入。如果需要下载SSL识别根证书，可直接在点击<点击下载SSL识别根证书>进行根证书分发到终端设备。

1. 使用系统内置根证书

[行为管理/策略高级选项/SSL证书设置]勾选使用系统内置根证书，点击<提交>。

2. 使用自定义根证书

[行为管理/策略高级选项/SSL证书设置]勾选使用自定义根证书。点击<去设置>按钮，进行自定义根证书配置，可选择三种自定义根证书的方式：生成新根证书、导入包含密钥的根证书、导入密钥独立的证书。

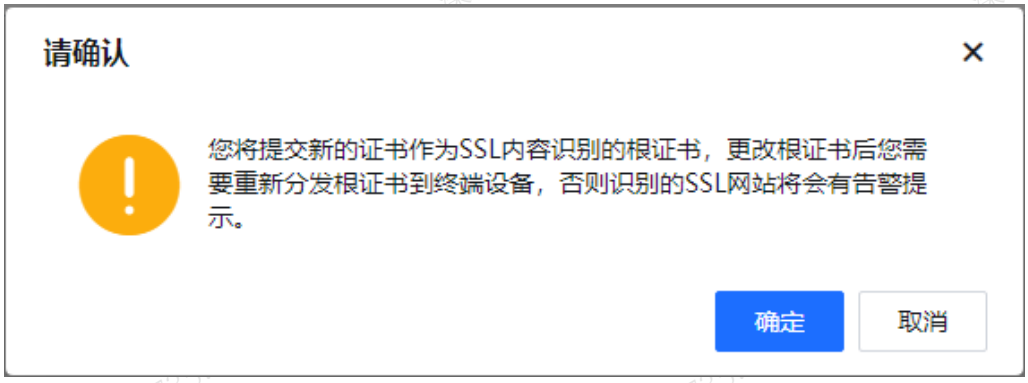
生成新根证书：需要填写的信息包括国家、省份、城市、公司、部门、颁发给、E-mail、密钥长度、证书编码、加密算法、有效期时间设置。

导入包含密钥的根证书：需要填写证书文件和加密密码。

导入密钥独立的证书：需要填写证书文件、私钥文件、加密密码。

返回配置界面后，提示“已设置自定义根证书，点击提交证书将会生效”，进行进一步确认。

点击<提交>，再确认，防止误操作，为终端带来麻烦。



确认<是>后，SSL证书设置界面提示证书状态“已生效”。

SSL证书分发

SSL证书分发功能需要安装根证书，可勾选<要求安装根证书>功能，对于未安装根证书的终端，将会重定向到证书安装页面，安装后用户才能正常上网。

（1）某单位的电脑是已经加入域控，然后通过域控组策略下发安装根证书。

（2）没有加入域控的电脑，推荐使用设备的[行为管理/高级选项/SSL证书分发]功能。

SSL证书实现原理：

- 每个终端上存在标记，是否需要检查根证书，是否已经通过检查。
- 如果需要检查且未通过检查，则会重定向到 。
- http://x.x.x.x/httpscert/https.htm?vlanid=xxx&url=xxxxxx&signver=xxxx,进行根证书检查，通过判断能否加载出checkcert.js判断是否安装了根证书。
- 如果通过检查则会发http://x.x.x.x/httpscert/handler，跳回本来访问的页面，比如百度。
- 如果检查不通过则会发http://x.x.x.x/httpscert/handler_failed，然后访问http://x.x.x.x/httpscert/index.html根证书下载页面。
- 如果切换根证书，则会把新的根证书md5下发，然后用户有流量过来的时候，就会把全局的根证书md5与用户本来的根证书md5做比较，如果不一样则会把通过检查的终端进行标记，重新进行SSL证书分发。
- 手动安装证书方式在PC端下载安装文件后，双击安装即可。

主备、多机情况下，所有根证书都同步。

BBC策略模板内置的根证书不会自动下发给各个分支AC的内置根证书，如需要下发需要手动导入。

只支持一级CA的根证书导入，不支持非一级CA证书及证书链功能。

认证策略为密码认证，终端访问任何域名都会先跳转到web认证界面，对于从未安装过设备根证书的浏览器，第一次认证通过后会跳转到证书安装界面，不会跳转到“认证跳转后”设置的页面；第二次认证时时如果已安装证书才会跳转到“认证跳转后”设置页面。

如果认证策略设置的是不需要认证或单点登录，此时终端上网可能并没有打开过网页就通过了设备认证，AC无法通过网页的重定向检查页面得知终端是否有安装过设备证书从而无法给终端推送证书安装页面、给终端用户打上终端证书检查通过的标记或放行标记；此时建议终端打开“安装SSL识别根证书”适用域名所填写的网页列表，通常打开常用的网页就能命中。

认证策略是不需要认证或单点登录时，为了提高终端用户打开网页重定向到根证书安装或检查页面的成功率也可以勾选“对80端口的HTTP请求强制重定向到证书安装页面”，但是如果终端用户上网时没有打开网页，此时如果终端后台程序有使用80端口通信那么一些应用会受到影响，所以最好建议每次上网前要打开一次网页。

上网时长排除应用列表

上网时长排除应用列表可以排除不需要统计的应用

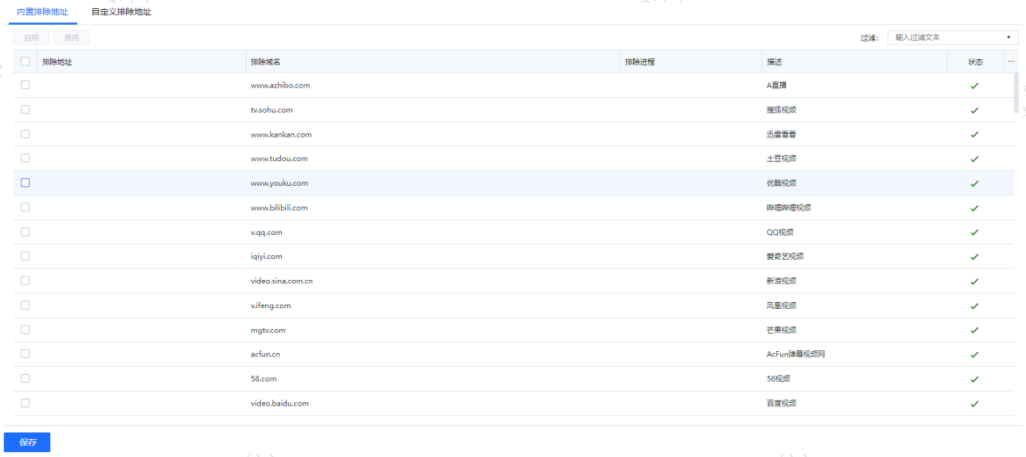
- 内置列表：**设备内置了一些如软件后台更新的应用流量，用户可以启用或者禁用这些内置软件列表。**

• 自定义列表：用户自定义需要排除统计和控制的应用。点击<选择应用>，选择需要排除的应用。如果列出的列表中，没有需要排除的应用，可以先到[对象定义/自定义应用]页面定义好需要排除的应用，然后再通过这里选择该应用进行排除。

• 排除端口：填写公网应用的目标端口，对该端口不进行时长审计和控制。

SSL解密全局排除

SSL解密全局排除支持内置排除地址和自定义排除地址两种方式。



说明

1．内置排除列表不能禁用和删除。

2．排除列表使用域名前缀方式进行排除，不支持通配符。

3．排除列表中的域名不会进行SSL内容解密。

4．域名排除列表需要能够正常进行DNS解析，才能正确进行排除。

分时访问设置

分时访问应用客户多网络场景，比如政务网和互联网，不能同时访问，需要实现访问互联网时无法访问政务网，访问政务网时不能访问互联网，用户可以自主进行网络切换，实现分时上网功能。

开启该功能需要勾选启用分时访问。

• 分时访问方式：web分时访问方式时用户访问到自定义网络触发切换，这时浏览器会重定向到切换页面；准入认证客户端分时访问方式时，用户可通过认证助手选择网络后直接关联策略。

• 拥有分时访问权限的用户：用来设置哪些用户具有分时访问的权限，可以选择所有用户或者自定义用户。

• 网络划分：主要用来设置不同的网络，需要自定义网络的名称、描述、IP地址或者URL，内置互联网是除了自定义网络之外的IP或者URL。

行为审计

随着企业办公网接入互联网，部分企业员工在办公时间会访问一些炒股网站、贴吧、论坛等，甚至会通过聊天软件、网站向互联网泄密公司内部机密资料。此时通过审计日志审计企业员工不规范行为尤为重要，且国家有关部门规定流程相关网络日志不少于6个月。深信服全网行为管理行为审计模块包括上网审计策略、客户端审计策略、业务审计策略、高级选项，通过多种审计策略对企业网络行为审计做到可视化。

管理员可对在上网审计策略、客户端审计策略、业务审计策略的页面进行删除、编辑、导入/导出、启用/禁用、上移/下移/移动到、过滤等操作，详细说明如下。

表22行为审计策略管理

操作	功能说明

删除策略	审计策略列表页面，可点击删除不需要的策略。
编辑/批量编辑	在审计策略列表页面，勾选需要编辑的审计策略，点击审计策略名称，设备会弹出审计策略的编辑页面，修改选中策略的相关信息。 批量编辑：勾选多个自定义的审计策略，可编辑策略的适用对象，其他信息不可以修改。
导入/导出	支持检查策略的导入/导出，选中自定义的策略然后勾选相应的策略，点击导出，即可将选中的策略导出，注意：内置的检查策略无法导出。点击导入，选中需要导入的检查规则文件，即可进行导入。
启用/禁用	选中已禁用的策略，点击启用，该策略即可生效，选中已启用的策略，点击禁用，该策略会失效。
上移/下移/移动到	由于策略是自上而下进行匹配，所以可以选中相应的策略，点击上移或者下移，或自定义移动，来进行优先匹配策略。
过滤	可输入需要过滤策略的名称，进行策略的过滤。

上网审计策略

上网审计策略包括应用审计、流量与上网时长审计和网页内容审计。

应用审计

应用审计用于对内网用户通过设备访问外网的行为和内容进行审计。审计对象包括Web邮箱、论坛、微博、Web网盘、笔记、HTTP外发与下载、网络协议、网络命令、其它、URL。以上应用类型可以在设备联网的情况下通过规则库更新。动作可选择审计或不审计。

类别	功能说明
Web邮箱	用于记录内网用户通过web邮箱发送邮件的行为。选择邮箱类型勾选对应的内容审计和附件审计后，可以记录内网用户发送邮件内容和附件。
论坛	用于记录内网用户访问论坛发帖的行为，根据需求勾选内容审计和附件审计。
微博	用于记录内网用户通过微博发送的信息的内容和附件信息，可审计新浪微博、腾讯微博、东方微博、皮皮时光机微博、Twitter等。
网盘	用于记录内网用户通过网页版百度云盘、钉钉网盘、OneDrive、Outlook网盘、微云、115网盘、Google Drice、ShareFile、WeTransfer、Dropbox等网盘上传的附件。

笔记	用于记录内网用户通过为知笔记、印象笔记、有道云笔记等笔记类应用上传的内容和附件以及百度文库上传的附件。
HTTP外发与下载	用于记录内网用户通过网页外发的内容和附件、通过网页下载的文件名。
网络协议	用于记录内网用户通过FTP协议上传及下载的附件、POP3/IMAP协议的内容和SMTP协议的内容。
网络命令	用于记录内网用户通过Telnet执行的命令，注意Telnet的端口必须是23号端口。
其他	勾选[其他网络应用]用于记录设备可以识别的网络应用行为； 勾选[未识别的网络应用]用于记录设备无法识别的网络应用行为，包括访问某个地址，某个端口等。因为设备无法识别这类应用，审计时会将访问的目标IP、端口等信息审计下来，会产生大量日志，所以建议不开启。
URL	用于记录内网用户访问网页的URL。勾选[URL]，点击[选择指定URL]用于指定URL类别，如果访问的URL属于选中类别的URL组，则访问的URL才会被记录。
生效时间	可审计全天、上班时间、下班时间，或者自定义的时间组。
文件类型	可选：电影、音乐、图片、文本、压缩文件、应用程序、Office系列、工程制造、娱乐音乐等。建议按需求勾选文件类型，否则审计的附件会占用较大的空间。

流量与上网时长审计

流量与上网时长审计用于设置是否统计组和用户的网络应用和域名的流量和时长。如果您选择了统计网络应用的流量和时长，那么您在设备的日志中心可以查询到内网访问公网的各种应用的流量和访问时间。勾选了统计域名流量和域名时长，则可以通过日志中心根据域名进行流量与时长统计。

• 记录每个组的网络应用流量：对经过设备访问外网的各种应用流量进行统计，可细化到组来进行统计和排名。若同时勾选[同时记录每个用户的网络应用流量]，则可根据用户来统计应用流量。该处配置是日志中心的应用流量统计和排行的基础，必须开启网络应用流量审计，才能在日志中心中查询关于应用流量的信息和排名。

• 统计域名流量：则会对经过设备访问外网的域名流量进行统计，可细化到基于域名来统计流量。

• 统计域名时长：则会对经过设备访问外网的域名时长进行统计，可细化到基于域名来统计上网时长。

• 记录每个用户的网络应用的时长：对经过设备访问外网的各种应用的上网时长进行统计。如果不勾选此项，则不会统计应用的上网时长包括总时长，在日志中心中查询不到关于上网时长的信息和排名。当勾选[忽略非人为产生的流量（如软件后台更新等）]：则在对经过设备访问外网的各种应用的上网时长进行统计时，将不会统计排除应用列表中的各种网络应用的上网时长。

点击<设置排除应用列表>将链接到窗口[排除应用列表]，它由“内置列表”、“自定义列表”和“排除端口”三部分组成。在“内置列表”中，定义了一些如软件后台更新的应用流量，用户可以启用或者禁用这些内置软件列表。在“自定义列表”中，用户可以点击选择应用来选择需要排除的应用。在“排除端口”中，可以填入需要排除不统计上网时长的端口。

说明：

记录每个用户的网络流量会产生更多的日志量，影响日志的查询、统计速度。在日志量太大的情况下，可以选择只记录每个组的网络应用流量，或者只对部分有需要的用户记录用户的网络流量，以获取更高的日志中心性能。用户数超过2W，建议不开启此功能。

网页内容审计

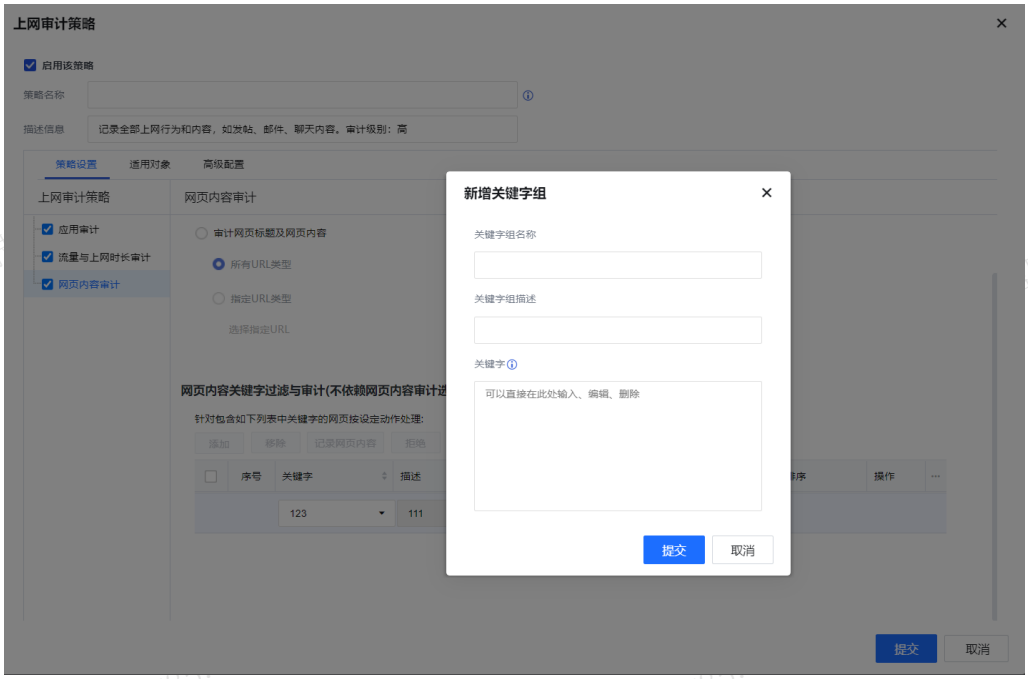
网页内容审计用于设置是否对内网用户访问互联网的网页内容进行审计。您可以通过此处的设置审计到所有网页的标题和网页内容，或者只审计指定URL类型的网页标题及网页内容。对网页中含有特定关键字的网页内容，可以设置拒绝、记录网页内容、记录并拒绝网页内容中含有特定关键字的网页。

- 不审计：当勾选时，设备不会记录访问网页的网页标题及内容。
- 审计网页标题及网页内容：分为所有URL类型和指定URL类型。

1)所有URL类型：设备将审计内网用户访问所有URL的网页内容和网页标题。

2)指定URL类型：设备只审计内网用户访问指定URL的网页内容和网页标题。

• 网页内容关键字过滤与审计：用于指定只审计网页中含有特定关键字的网页内容，过滤网页中含有特定关键字的网页。



• 关键字：选择需要生效的关键字组或新增关键字组。

• 生效时间：选择检测此类关键字的生效时间。

• 动作：选择检测到此类关键字时设备的处理方式：有记录网页内容、拒绝和记录网页内容并拒绝三种选项。

说明：

1．指定关键字存在并且动作包含记录网页内容时，设备会将相应的网页标题及网页内容都记录下来；指定关键字存在并且动作为拒绝时，则会将网页内容拒绝。

2．上网审计策略可以通过[系统管理/系统配置/授权管理]多功能序列号控制行为审计与内容审计的分离，从低版本升级上来的设备默认开启的是内容审计。序列号只开启行为审计时，控制台界面的上网审计策略中将无法看到“内容审计”模块。

3．当设备内存占用超过70%会消耗较大性能，建议在无此需求的时候不启用该功能。

上网审计配置案例

需求场景

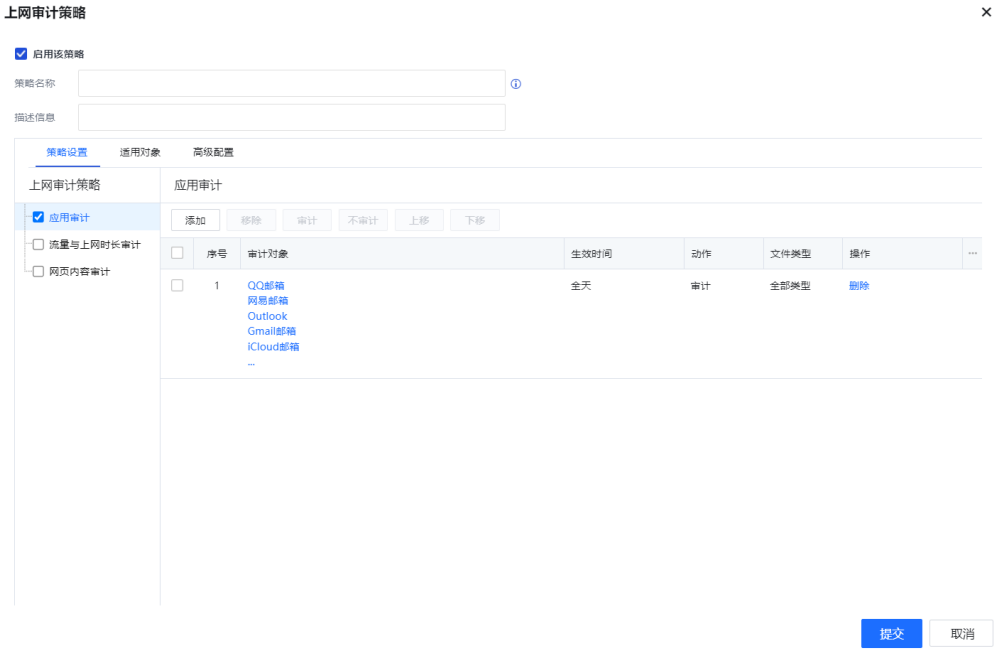
设置一条审计策略审计微博所发的文本信息和图片信息、审计Webmail邮件和其附件内容、审计用户访问网页和通过网页下载的文件名称、审计各类已知应用的行为实例策略。

操作步骤

步骤1.在[行为审计/上网审计策略]新增上网审计策略，填写[策略名称]和[描述信息]，勾选[应用审计]，点击<添加>按钮，在弹出的[选择审计对象]窗口选择需要审计的对象。

步骤2.在策应用审计添加审计对象，勾选审计对象Web邮箱、论坛、微博、HTTP外发与下载、URL等。并

设置[生效时间]为全天，[动作]为审计，[文件类型]为全部类型。点击<确定>按钮。



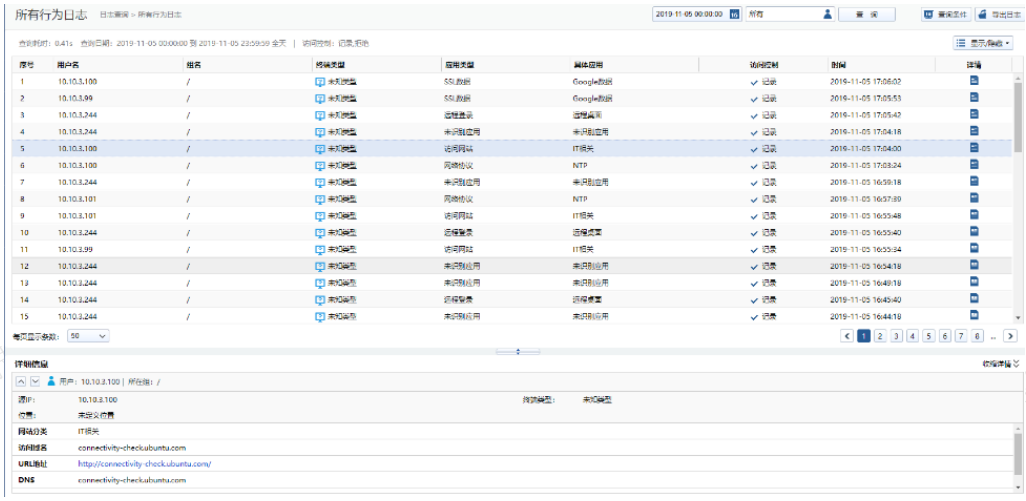
步骤3.选择[适用对象]，此处选中的用户组和用户将全部匹配此审计策略，点击<提交>按钮完成策略配置。

步骤4.设置[高级配置]，高级配置中包含策略过期日期设置、同级别管理员查看编辑权限设置、允许低级管理员查看。

步骤5.由于部分网站为https加密网页，部分WEB邮件使用SMTP、POP3等协议，需要配合[行为管理/SSL解密策略]进行解密来审计，详细配置请参考新增SSL解密策略章节。

步骤6.点击<提交>配置完成，用户在浏览器上访问新浪微博并发送一条包含文字和图片的微博动态。

步骤7.效果展示，点击设备右上角[日志分析平台]下拉框中的[进入日志中心]进入日志中心中的[日志查询/所有行为日志]查询相关审计日志。



说明

：

1.当需要审计https形式加密的行为和内容需要结合[行为管理/SSL解密策略]使用。

2.此种场景开启中间人解密会影响全网行为管理设备性能，开启需注意。

客户端审计策略

客户端审计策略主要包括客户端应用审计、外接设备审计、打印机审计、浏览器外发审计。

说明：

1.客户端审计策略需要PC安装准入客户端才能生效。

2.准入客户端目前只支持Windows系统。

3.配置外接设备审计策略需要开启终端接入安全序列号。

4.配置打印审计审计策略需要开启防泄密外发审计授权。

客户端应用审计

客户端应用审计包括内置终端应用识别库（IM、邮件客户端、网盘应用、办公软件、笔记软件、会议软件、网络传输工具、远程工具、运维工具）和自定义应用库（参考10.1.3.2. 自定义终端应用库章节）。内置终端应用识别库可联网进行更新。

• IM：通过准入客户端的方式审计终端IM即时通讯工具的聊天内容和传输的文件，个人版QQ、个人版微信、Viber、WhatsappMessenger、Skyper企业版仅支持审计文件，不支持审计聊天内容。

• 邮件客户端：通过准入客户端的方式审计内网用户使用邮件客户端发送邮件附件。

• 网盘应用：通过准入客户端的方式审计内网用户使用网盘应用上传文件。

• 办公软件：通过准入客户端的方式审计内网用户使用办公软件上传文件。

• 笔记软件：通过准入客户端的方式审计内网用户使用笔记软件上传文件。

• 会议软件：通过准入客户端的方式审计内网用户使用会议软件上传文件。

• 网络传输工具：通过准入客户端的方式审计终端通过文件传输类工具传输的文件。目前包括WinSCP、XFtp、FileZilla三种文件传输工具。

• 远程工具：通过准入客户端的方式审计终端通过远程类软件传送的文件。目前包括Todesk、向日葵、AnyDesk三种远程类软件可选。

• 运维工具：通过准入客户端的方式审计终端通过运维类工具发送的文件。目前包括XShell、MobaXterm两

种运维工具。

- 动作：可选审计、不审计。
- 生效时间：可选上班时间、下班时间、全天，也可以自定义时间计划。
- 文件类型：可过滤文件类型，文件类型可在[系统管理/对象定义/文件类型组]中定义。
- 离线审计：支持开启离线审计（即支持准入客户端与AC断开连接的情况下审计）。
- 附件审计：可选择启用、禁用。启用后会同步保存日志附件，禁用后仅记录行为。
- 外发截屏：支持开启外发截屏，对文件外发时刻的整个桌面屏幕进行多次截屏。

说明

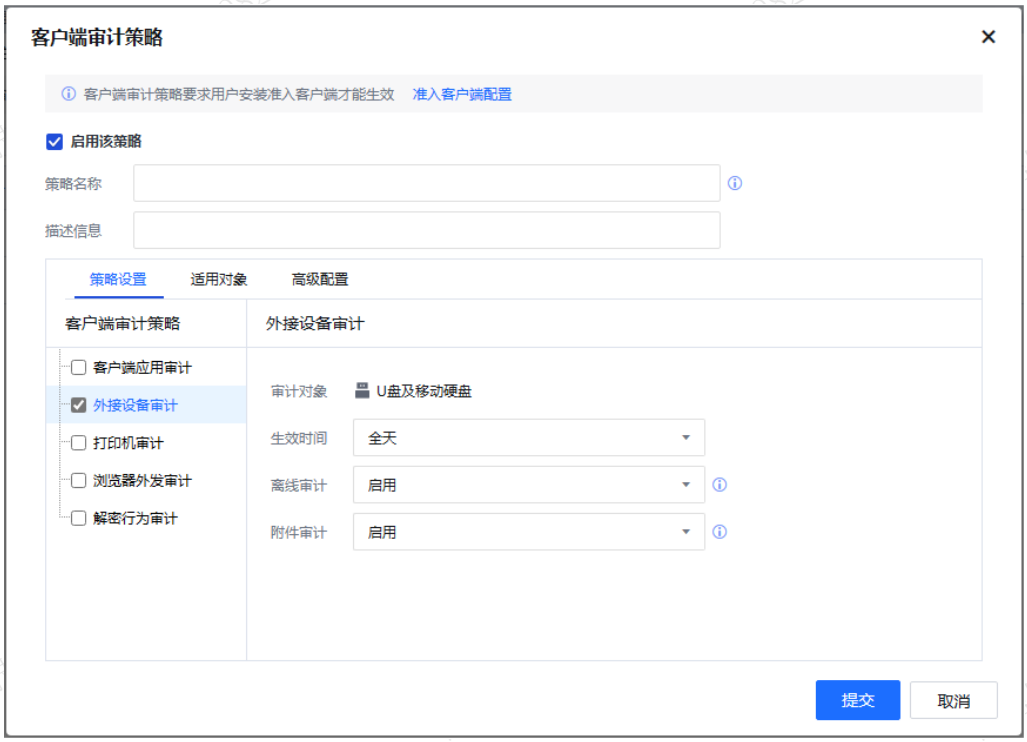
：

1.外发截屏是审计文件外发的增强型功能，文件审计后，在日志中心的文件审计日志中除了可以查询外发的文件外，还可以查询到文件外发时刻的屏幕截屏。

2.离线审计需要终端已经接入过AC并获取到相应的策略才会生效。

外接设备审计

外接设备审计可勾选移动存储介质和离线终端审计。



- 生效时间：可选上班时间、下班时间、全天，也可以自定义时间计划；
- 离线审计：支持准入客户端与AC连接断开的情况下审计（笔记本带离公司的情况）。
- 附件审计：可选择启用、禁用。启用后会同步保存日志附件，禁用后仅记录行为。

点击<准入客户端配置>会跳转到准入客户端配置页面，详细配置在[接入管理/终端管理/准入客户端配置]参考准入客户端配置章节。

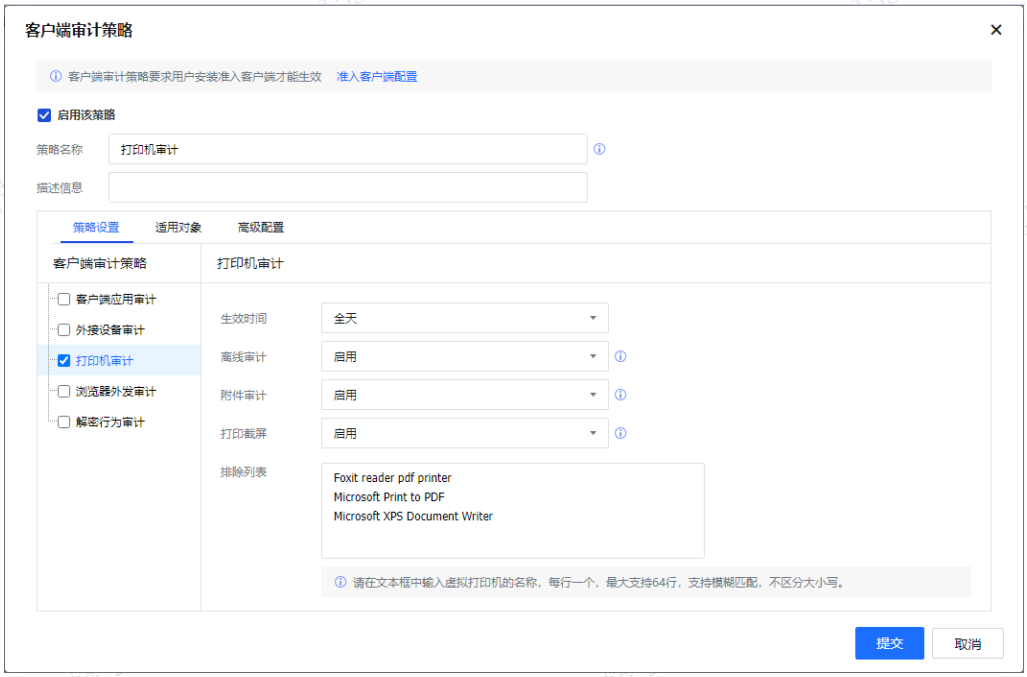
说明

：

离线审计需要终端已经接入过AC并获取到相应的策略才会生效。

打印机审计

打印机审计支持对用户的打印环节进行全程审计，包含用户名、时间、打印文件信息（文件名、文件类型、文件大小、文件数、文件页数）、打印机型号、打印机名称、打印应用程序等都会全程跟踪记录。

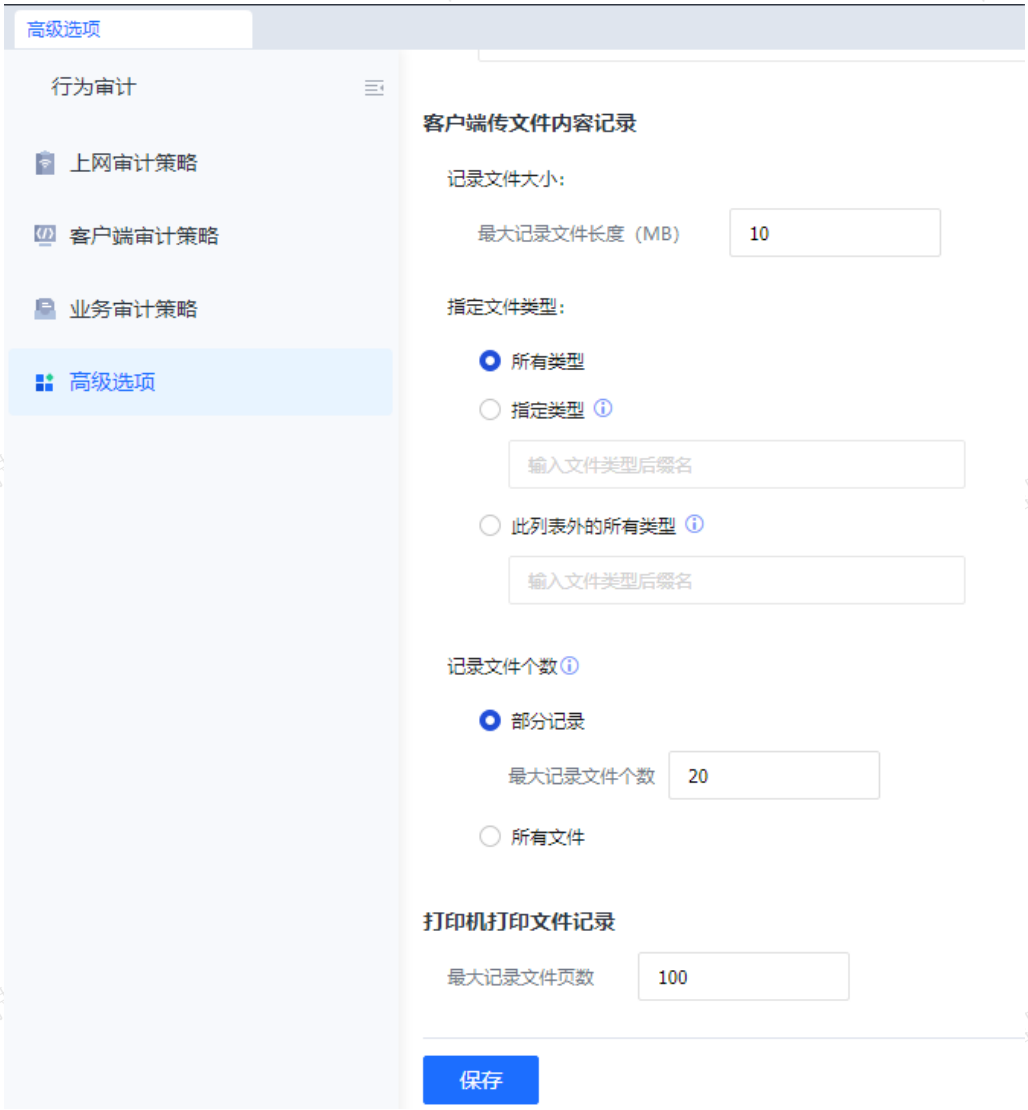


- 生效时间：可选上班时间、下班时间、全天，或自定义时间计划。
- 离线审计：支持离线终端审计，准入客户端与AC连接断开的情况下仍支持审计（用户终端离网场景）。
- 附件审计：启用后审计打印附件，禁用时仅记录打印行为。
- 打印截屏：启用后对触发打印文件动作时，对打印时刻的整个桌面屏幕进行一次截屏。
- 排除列表：填入不需要审计的打印机设备名称。排除列表中默认排除常见的3种虚拟打印机，虚拟打印机是一种软件，用于模拟实现打印机功能，通常将打印文件以某种特定的格式保持在电脑。

说明：

打印机审计目前只支持Windows 7及以上非Windows server版本操作系统。

单次打印最大支持审计页数500页，默认100页。



打印应用程序支持列表 (支持在线规则更新)

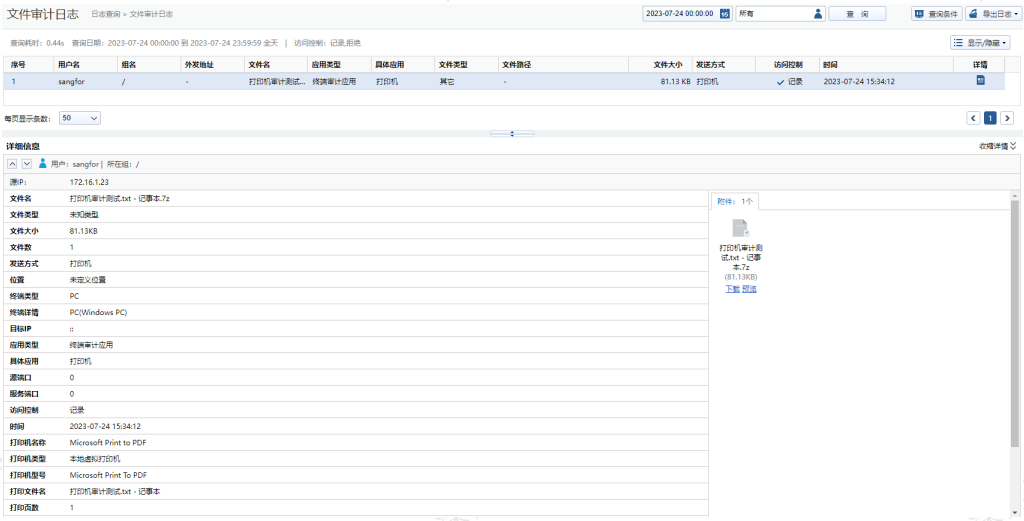
打印类型	打印应用程序
PDF	Chrome
	Edge
	Safari
	Firefox
	福昕阅读器
	Adobe Acrobat Reader
	Microsoft office
	WPS office
	WPS文本

Word、Excel、PPT(WPD office)	WPS表格
	WPS演示
Word、Excel、PPT(Microsoft office)	Word
	Excel
	PowerPoint
图片	WPS图片查看
	Windows自带截图工具
	Snipaste截图打印
	Photoshop
云笔记	有道云笔记
	印象云笔记
文本	Notepad
	Notepad++
	Xmind
	Vscode
	pycharm

打印机审计效果

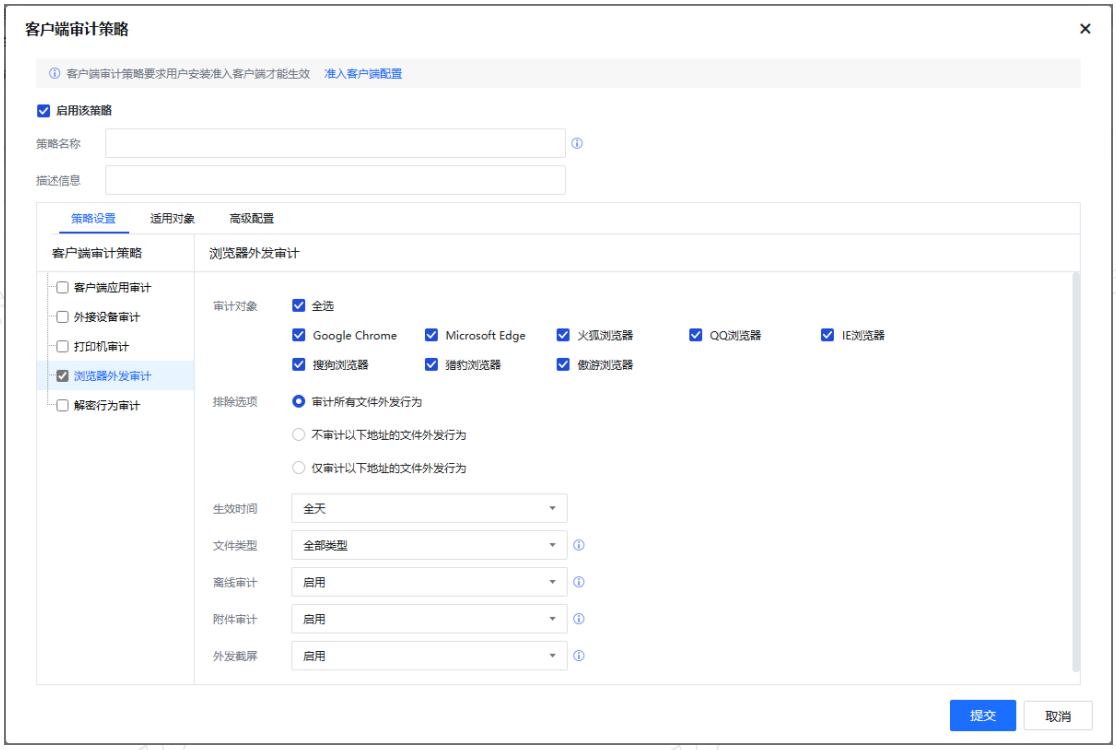
1. [全网监控/上网行为监控]可实时查看打印行为的基本信息(打印文件名、应用程序、打印机名称)。

2. 日志中心[所有行为日志]或[文件审计日志]中可查看打印审计详细信息，可以下载或在线预览审计内容。



浏览器外发审计

浏览器外发审计基于准入客户端实现审计终端外发文件。



审计对象：选择需要审计的浏览器，目前支持Google Chrome、Microsoft Edge、火狐浏览器、QQ浏览器、IE浏览器、搜狗浏览器、猎豹浏览器、遨游浏览器。

排除选项：审计所有文件外发行为；不审计以下地址的文件外发行为（除以下地址外，审计所有）；仅审计以下地址的文件外发行为（只审计以下地址，其余地址不审计）。

生效时间：可选上班时间、下班时间、全天，或自定义时间计划。

文件类型：可过滤文件类型，文件类型可在[系统管理/对象定义/文件类型组]中定义。

离线审计：支持离线终端审计，准入客户端与AC连接断开的情况下仍支持审计（用户终端离网场景）。

附件审计：可选择启用、禁用。启用后会同步保存日志附件，禁用后仅记录行为。

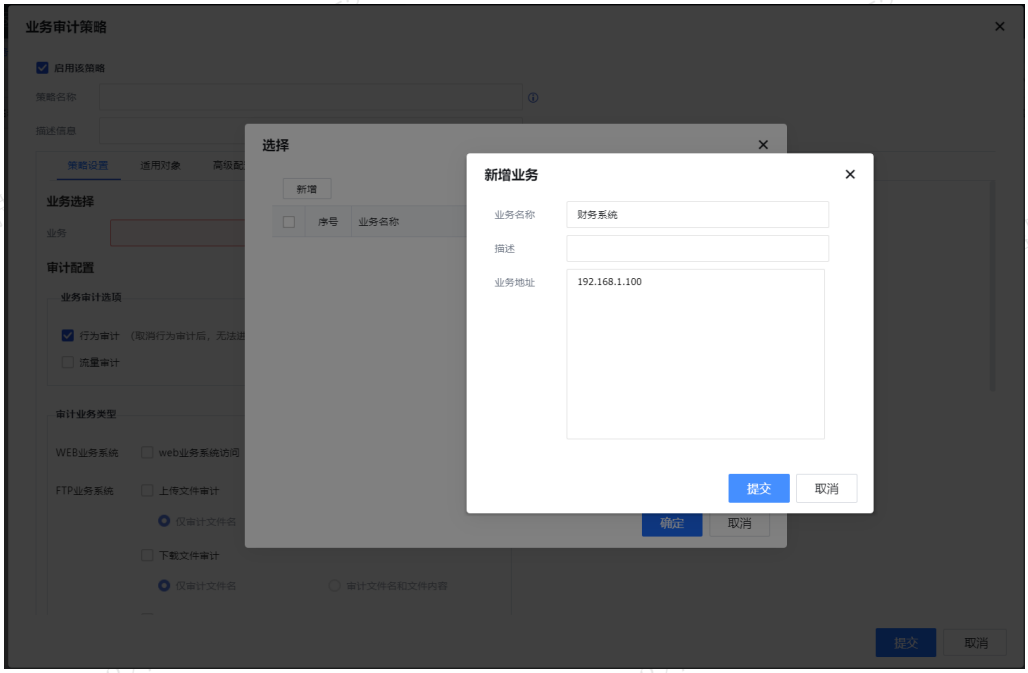
外发截屏：支持开启外发截屏，对文件外发时刻的整个桌面屏幕进行多次截屏。

业务审计策略

业务审计策略可以帮助管理员了解什么用户、用了什么账号、访问了什么业务系统，上传或下载了哪些文件，从而更好地管理企业的业务系统和规范用户的行为。

业务审计支持的业务类型主要有Web业务系统、FTP业务系统和SMB业务系统，可以记录用户对这些业务系统的访问、上传文件、下载文件等动作以及记录相关文件，还可以对服务器的外联行为进行记录。

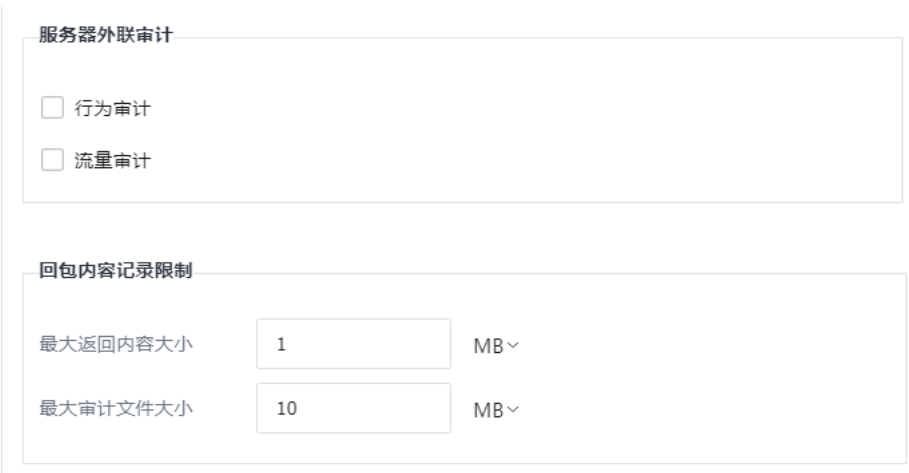
业务选择：可以选择事先自定义好的业务或者直接新增业务，以便对该业务审计。



业务审计选项：可以审计业务访问的数据，包括行为和流量审计（取消行为审计之后无法进行业务系统审计和分析）。

审计业务类型：用来选择审计的业务，包括WEB业务系统、FTP业务系统、SMB业务系统。其中FTP和SMB可以精细化配置。支持独立选择上传文件、下载文件、其他行为，上传和下载支持选择仅审计文件名或者审计文件名和文件内容。

- WEB审计：登录账号，登录密码（不支持加密），登录状态，文件上传，文件下载、自定义动作审计。
- SMB审计：用户登录/注销，删除目录，重命名目录，上传文件，下载文件，重命名文件，删除文件。
- FTP审计：用户登录/注销，创建目录，删除目录，重命名目录，上传文件，下载文件，重命名文件，删除文件。



服务器外联行为审计：可以对服务器外联情况进行审计，包括行为和流量审计。

回包内容记录限制：最大返回内容大小最大为50MB，最大下载文件大小最大也为50MB。

说明：

1.SMB业务审计只支持v1、v2，不支持v3。

2.业务SSL加密场景注意事项：

(1).内网访问业务需要开启SSL解密；

(2).外网用户访问业务场景需要配合AD开启SSL卸载。

业务审计配置案例

需求场景

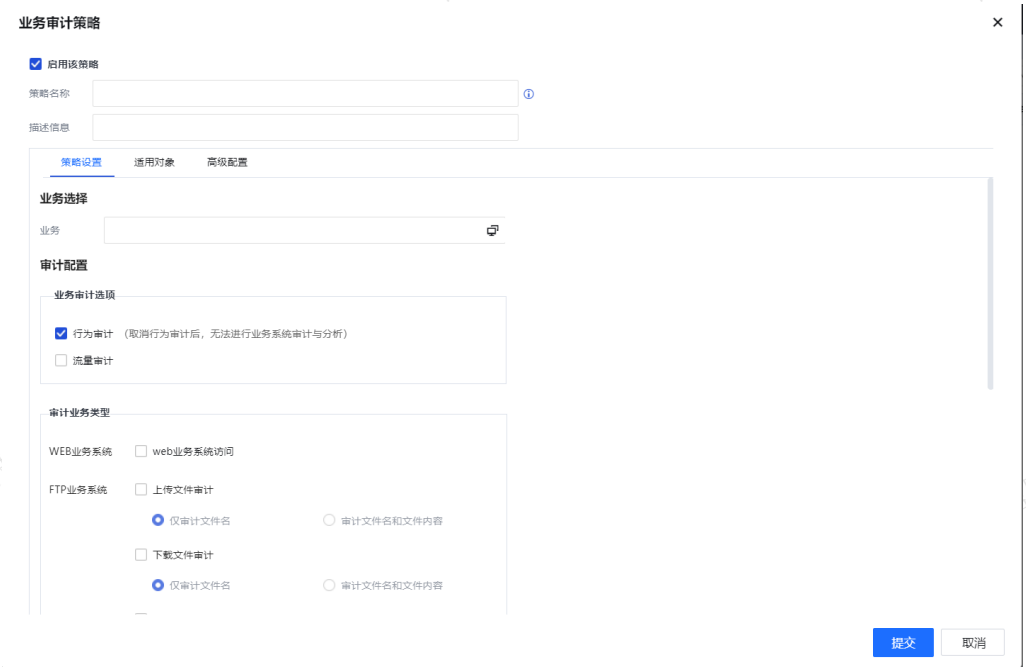
某企业需要对公司的FTP、SMB和WEB业务系统的流量进行审计，记录用户对业务系统的所有操作行为及文件，从而更好地管理企业的业务系统和规范用户的行为。

配置步骤

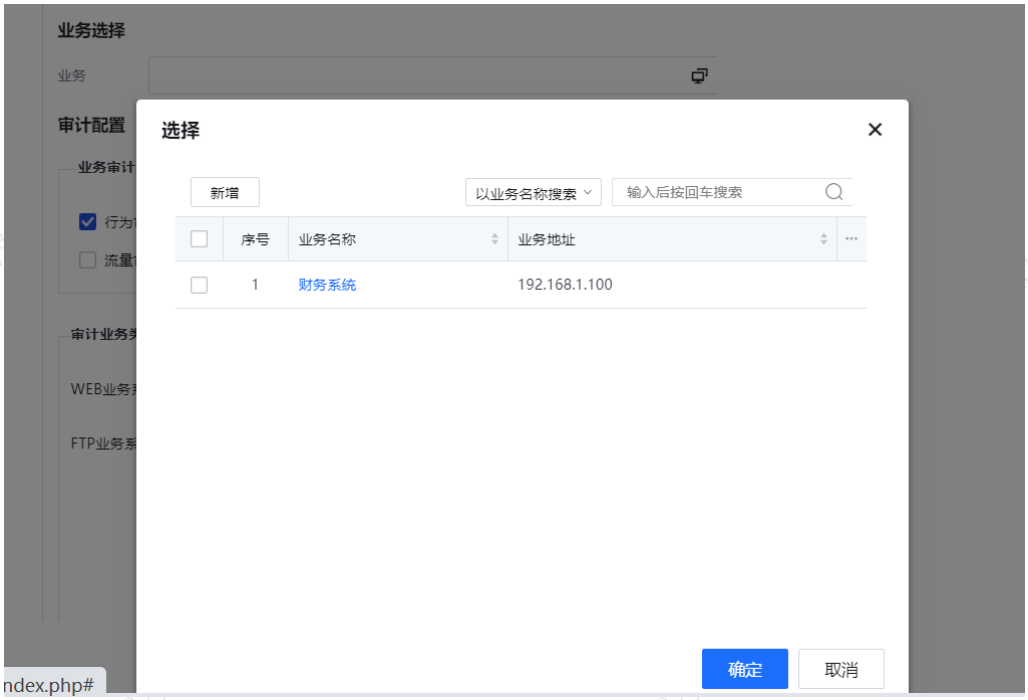
步骤1.在菜单栏[行为审计/业务审计策略/业务定义]点击<新增>，然后填写业务系统的名称及业务地址信息，依次新增好FTP、SMB和WEB系统的信息。

步骤2.在菜单栏[行为审计/业务审计策略]点击<新增>，然后选择[业务审计策略]，进入新策略编辑界面。

步骤3.勾选[启用该策略]，开启该策略。填写策略名称。



步骤4.点击[业务选择/业务]，选择定义好的业务，点击<确定>回到策略编辑页面。



步骤5.根据需求勾选[审计配置/业务审计选项]中的行为审计；

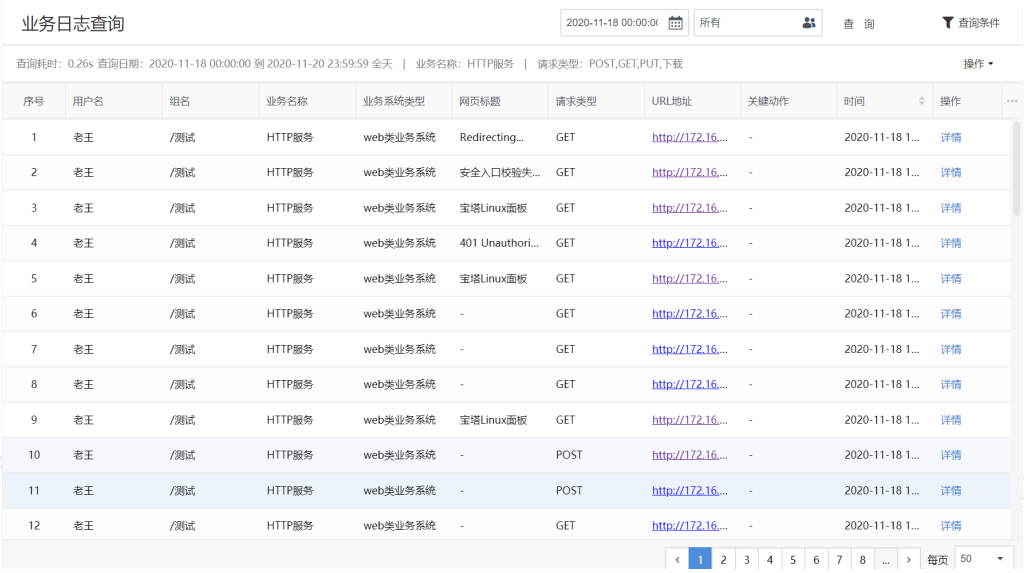
步骤6.设置[适用对象]，此处选中的用户组和用户将全部匹配此上网策略设置的审计策略。

步骤7.设置[高级配置]，高级配置中包含策略过期日期设置、同级别管理员查看编辑权限设置、允许低级管理员查看。

步骤8.点击<提交>完成策略配置。

步骤9.用户终端使用资源管理器访问FTP系统和SMB系统，并进行文件上传和下载；使用浏览器访问WEB业务系统进行登录操作。

步骤10.点击界面右上角[日志分析平台]，点击[业务审计]应用，点击[日志查询/业务访问日志]，可以看到用户对业务系统进行了哪些操作。



步骤11.点击[详情]可以看到该用户使用了什么账号对该业务系统进行了什么操作以及审计到的文件。

高级选项

日志记录用于设置设备审计访问网站日志和准入IM传文件内容记录的详细程度，包括日志记录、 审计过滤规则和准入IM传文件内容记录。

访问网站日志记录选项：

• 优化日志记录：仅记录文本类型的web网页，且短时间内访问同一个域名只记录一次。

• 仅记录到网站根目录的访问：只记录对根站点的访问日志。

• 记录所有网页访问：设备会记录所请求网页的每个元素，勾选此项会产生大量日志，一般不推荐使用。勾选[但不记录以下类型的访问]，则不记录填入对话框内的特定文件后缀的访问请求，有多个文件类型请用逗号隔开。

其他日志记录选项：

• 记录源MAC：将会记录日志的源MAC地址。

• 记录VLAN_ID：将会记录日志的VLAN ID。

审计过滤规则：

• 不审计含有如下前缀的URL（一行一个前缀），不记录含有填入对话框的前缀的URL，支持模糊匹配，不支持通配。

• 不审计含有如下后缀的URL（一行一个后缀），则不记录含有填入对话框的后缀的URL，支持模糊匹配，不支持通配。

准入IM传文件内容记录：

• 记录文件大小：用于设置通过准入方式审计IM传文件的文件内容时，记录文件的最大长度。当用户发送的文件超过了这个设置的值，那么审计的文件将仅记录用户设置的大小，其余部分将被截断，但可以通过数据中心的外发文件查询查询到该文件是否被截断以及文件的原始大小。设备能够记录的最大文件长度为500MB。

• 指定文件类型：用于设置通过准入方式审计IM传文件的文件内容时，记录文件的文件类型。

• 所有类型：表示记录客户端所发送的所有类型文件。

• 指定类型：表示仅记录用户填写类型的文件。

• 此列表外的所有类型：表示仅记录填写类型之外的所有文件类型。这些类型仅仅是文件的扩展名，对于没有扩展名的文件，只有选择“所有类型”或者“此列表外的所有类型”才能进行记录。

说明

当QQ客户端以文件夹的形式发送文件时，若文件夹中包含的文件数量超过20个，则仅随机挑选其中的20个文件来进行记录。

安全管理

随着平板、手机等智能终端的流行，在无线和固网混合的网络环境下，有些公司内部员工可能私搭无线AP（Access Point），通过无线AP到公司网络出口，这些AP由于安全措施薄弱，极容易被外人破解，可能导致内网暴漏，信息安全遭受威胁。

通过安全管理功能也可以避免部分员工通过代理软件上网，规避权限控制，给内网管理造成漏洞和风险。安全管理功能可帮助用户实现不同终端接入网络的管理，识别无线智能终端等设备通过私搭AP接入以及终端的代理上网行为，防范无线智能终端设备接入引起无线安全漏洞导致泄密。

终端防私接

共享接入管理

共享接入管理用户检查内网代理他人上网的行为，可以设置单IP和单用户的最大上网的终端数。当检测到共享上网行为超过设置最大终端数时，可以冻结此IP或用户。

在[安全管理/终端防私接/共享接入管理]，点击启用共享接入检测，可以开启共享接入检测功能。

注意

1.为增强防共享终端识别效果，建议在[全网监控/发现设置/终端识别设置]启用全网终端识别功能，如需要对违规终端进行冻结操作，则必须启用终端识别功能。

2.AC设备CPU利用率超过70%则不建议开启终端识别功能。

点击<配置选项>可以设置共享接入的检测配置，统计方式和自动冻结检测配置。

其中：

• 选择统计所有终端，自动冻结可设置终端数量达到多少台以上，冻结多少分钟，还有允许例外情况（满足以下条件时不会被冻结）：设置单个IP可以允许电脑终端数和移动终端数。冻结选项可选冻结IP地址或者冻结用户名。

• 选择仅统计电脑终端（只包含windows和mac），自动冻结只能设置终端数量达到多少台以上，冻结多少分钟，冻结选项可选冻结IP地址或者冻结用户名。

• 冻结选项使用场景

冻结IP地址：常用于企业用户，即使是公共账号也仅冻结私接的个人，当检测到共享接入后，拒绝来自该IP的所有上网数据。

冻结用户名：常用于高校或运营商，防止用户重新拨号逃避冻结，当检测到共享接入后，拒绝该用户名的所有上网数据。

说明：

如果是高校场景，可勾选“存在校园网破解版路由器时”，校园网破解版路由器又称“黑路由”，可对此这类型的设备进行检测和冻结，从而提升高校网络运营者发现共享行为的能力。校园网破解版路由器不受终端检测数量的限制，只要检测到校园网破解版路由器即认为是共享终端，立即执行冻结动作。

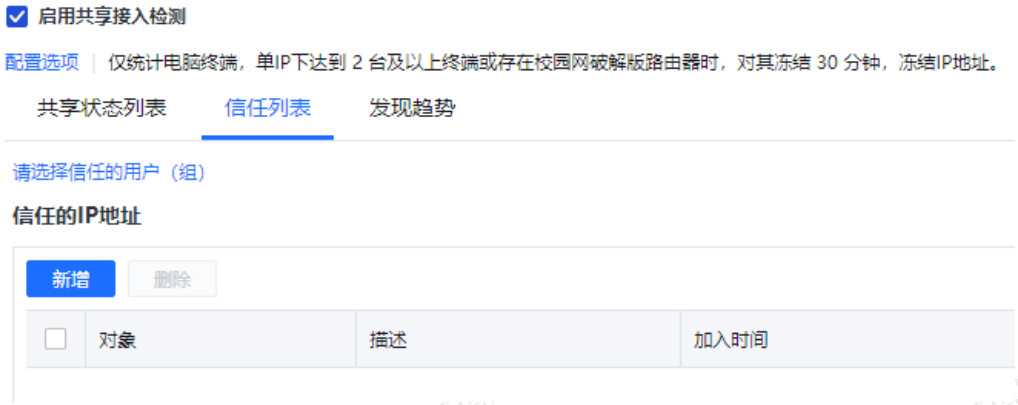
共享状态列表

主要显示当前通过共享方式接入网络的IP地址和用户信息，可选择点击<冻结>、<解冻> 用户，选择相应的用户标记为信任。

点击<过滤条件>可设置筛选类型：所有用户、已冻结用户、未冻结用户。或根据IP地址进行筛选过滤。

信任列表

当管理员加入信任列表的用户、用户组和IP后，不做接入共享检测，点击<新增>信任的IP地址和IP范围，加入到信任列表的IP地址将不进行防共享检测。



点击<请选择信任的用户（组）>会跳转到组织架构，选择信任的用户和用户组。
在信任的IP地址栏，点击<新增>，可在IP输入框，输入IP地址，则该IP会加入到信任列表且不会进行防共享检测。

点击<提交>完成配置。

发现趋势

可以选择统计最近7天或者最近30天共享上网的用户数。统计方式有：按源IP统计、按用户名统计。如果想要查看更多共享上网的用户信息，可点击<日志中心>进行查看。

移动终端管理

移动终端用于检测和封堵不受信任的移动终端接入网络，通过流量特征来识别移动终端，如果AP是NAT模式，则发现的是AP的IP，如果是非NAT模式，则发现的是移动终端的IP。

在[终端行为安全/终端防私接/移动终端管理]，点击启用移动终端管理，可以开启移动终端发现功能。

注意

1.为增强移动终端识别效果，建议在[全网监控/发现设置/终端识别设置]启用全网终端识别功能，如需要对违规终端进行冻结操作，则必须启用终端识别功能。

2.AC设备CPU利用率超过70%则不建议开启终端识别功能。

点击<编辑配置选项>，打开移动终端管理配置选项，当发现新移动终端后的行为可以是冻结此移动终端上网或者是发送邮件告警。若未勾选“冻结此移动终端上网”，只统计移动终端数量，不执行冻结动作。

发送告警邮件：点击<配置告警选项>，自动跳转到告警选项页面进行设置。为了确保高级能正常发送，需保障邮件能正常使用。详细配置参考告警选项设置。

冻结此移动终端上网：可以自定义冻结时间。

移动终端列表

显示接入的移动终端的IP、用户名、所属组、终端类型、详情、状态以及最近发现时间等信息。

移动终端发现通过流量特征来识别移动终端，如果AP是NAT模式，则显示的是AP的IP；如果是非NAT模式，则显示的是移动终端的IP。移动终端列表的详情会显示出通过UA规则识别的具体应用名称。

点击<导出列表>，将移动终端列表中的条目导出至csv文件，导出的内容和格式与移动终端列表相同。

移动终端列表页面最多显示一周内的1000条数据，如果有更多的数据，可以点击<日志中心>跳转到日志中心页面，点击<终端接入分析>页面进行查询更多日志。

信任列表

用于添加管理员允许接入的移动终端，来自信任列表里面的移动终端，设备不会拒绝他们上网。点击<请选择信任的用户（组）>会跳转到组织架构，选择信任的用户和用户组。
在信任的IP地址栏，点击<新增>，可在IP输入框，输入IP地址，如果是AP做的无线路由器，直接输入AP的IP，如果是AP做的无线网桥，填上AP做的DHCP的网段。加入信任列表的移动终端将不回再出现到终端列表中。

点击<提交>完成配置。

发现趋势

用于统计最近7天或者最近30天的移动终端个数，如果有更多的数据，可以点击<日志中心>链接到移动终端管理页面进行查询。

终端防翻墙

终端防翻墙是用于检测和封堵内网终端用户使用代理工具上网。在[安全管理/终端防翻墙]，点击启用代理工具检测功能，可以检测内网是否有使用代理工具，但是不拒绝该代理工具，不开启则不检测。如果需要对使

用代理工具的用户进行惩罚措施，那么需要在[配置选项]里配置对应的惩罚措施。

点击<配置选项>会跳转到代理工具管理配置选项，其中包括需要惩罚的代理工具配置、封堵策略、排除列表。

点击<代理工具>会跳转到代理工具应用页面，可选择具体需要惩罚的代理工具。

在封堵策略可设置封堵手段，包括联动EDR封堵、流量封堵、封堵下载路径

EDR联动封堵

使用EDR联动封堵处置时，需要在[安全管理/终端上网安全/安全配置/终端检测和响应（EDR）]完成和EDR联动。

联动EDR后，AC下发对应的代理软件列表到EDR，当EDR检测到终端运行代理软件时，可以对终端的代理软件进行封堵，解决通过网络侧对代理软件封堵效果不佳的问题。

当EDR检测到终端存在代理软件在运行，立即进行封堵，并弹窗告警，如下图。

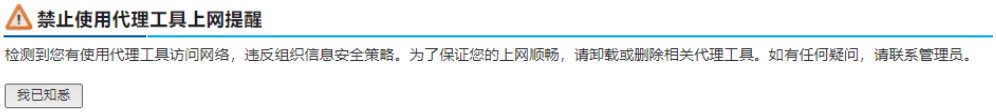
说明

使用[EDR联动阻断违规代理]是需要先配置联动EDR相关参数，只有联动正常才能通过EDR对相关的代理工具进行封堵。

流量封堵

在[流量封堵违规代理]配置内可以选择提醒违规使用代理软件的用户，或者选择惩罚违规使用代理软件的用户。两种方式可以分开使用，也可一起使用。

提醒代理工具用户：点击<预览>可以预览到被拒绝提示的页面，如需要修改此页面，可在[系统管理/系统配置/终端提示页面制定/其他页面]中修改相应的页面即可。



惩罚用户：管理员设置被惩罚的用户在惩罚的时间内将用户添加到惩罚通道和禁止该用户上网。可选择设置惩罚时间为30分钟，且添加到惩罚通道。惩罚通道的详细配置可参考惩罚通道章节。也可选择设置惩罚时间为30分钟，且禁止该用户上网。当惩罚时间过后，将会重新检测，如果该用户还继续适用代理工具，会继续被惩罚。

封堵下载路径：在AC内置的规则库中相关的代理软件（代理工具选择页面的软件）已经关联了对应的软件官方下载地址，勾选[封堵所选应用的官网下载地址]后用户无法去官网下载对应的软件程序。也可通过[封堵自定义地址]来封堵其他的下载地址，自定义支持填写IP和域名，域名支持泛域名格式输入。

DNS地址排除列表：DNS服务器在内网时，开启封堵策略可能会导致DNS功能失效，所以管理员可在DNS排除列表输入需要排除的DNS服务器地址。

白名单列表

填写需要排除的代理工具的目的IP或者域名，当用户再次访问此IP或者域名时不会再判断为使用代理工具。

代理工具列表

显示被检测到使用代理工具终端的IP、用户名、所属组、终端类型、代理工具名称、状态、发现时间等信息。

代理工具列表页面最多显示一周内的1000条数据，如果有更多的数据，可以点击<数据中心>链接到移动终端管理页面进行查询。

信任列表

用于添加管理员允许使用代理工具的终端，来自信任列表里面的终端，设备不会拒绝他们使用还代理工具。

信任的用户：可以添加受信任的用户或者组，点击<请选择信任的用户(组)>会跳转到组织架构，选择信任的用户和用户组。点击<新增>信任的IP地址和IP范围，点击<提交>。加入到信任列表的IP地址将不会在代理工具类别中。

代理工具趋势

用于统计最近7天或者最近30天的使用代理工具的终端个数，管理员还能按次数统计和按用户统计。

终端上网安全

终端上网安全是从内容安全、终端安全和网络安全三个方面为上网提供安全防护能力，立体式提供整体的网络安全服务。

安全防护能力

在[安全管理/终端上网安全/安全防护能力]页面主要呈现安全能力图谱、安全能力更新指标、能力更新日历等信息。

安全能力图谱

设备和安全云脑联动，构建立体的威胁防护体系。接入深信服安全云脑后，可以获得海量且多维度的威胁情报、SAVE安全智能检测引擎多重抓紧规则引擎、实时云端检测技术、大数据智能分析和检测以及高实时的云端协调能力。结合设备，从终端安全、内容安全和网络安全三个角度立体化的为您提供上网安全服务。

图中，已经启用的功能显示为绿色勾选状态，点击可以跳转到对应的配置页；未启用功能显示为灰色未勾选状态，点击亦可跳转到对应的页面进行配置。

安全能力概况

安全能力更新指标：概要说明设备的安全能力。

威胁响应最快完成时间：最近一个月所有新的威胁从爆发到设备更新检测防御能力中的最短时长。

云查杀次数：显示设备接入云脑后，最近一个月平均每天云查杀的次数。

安全事件总数：最近一个月安全事件数。

安全能力云更新趋势：一个月内的安全能力云更新趋势。

全网实时热点事件TOP10：全网最热门10个事件。

能力更新日历

显示一个月内安全能力更新情况，无更新显示“更新0”；有更新的时间，鼠标落在更新条目上可以看到具体更新的内容和更新量，包括URL规则库、恶意链接规则库、应用识别规则库、僵尸主机规则库及热点时间更新，会在当天显示更新项和数量。

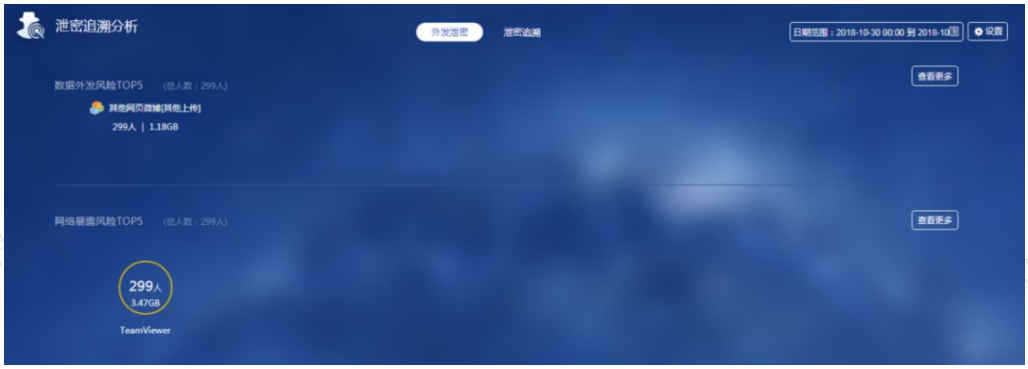
安全配置

在[安全管理/终端上网安全/安全配置]，配置内容安全、终端安全、网络安全功能，页面如下。

内容安全

泄密风险：深信服防泄密事前准确识别风险用户，事中监控敏感数据并及时告警，事后进行泄密追溯与分析，全面保障用户信息安全，避免信息泄露造成的损失。

点击<防泄密追溯应用分析>按钮，能跳转到日志分析平台-泄密追踪分析应用，查看分析的结果。



泄密风险检测功能需要联动日志分析平台使用。

1. 配置上网审计策略。
2. 如果使用内置日志分析平台，第一次需要进入内置日志分析平台，启用泄密追踪分析应用。
3. 如果使用外置日志分析平台，保障设备和外置日志分析平台可以正常通信（TPC810和801端口），勾选[系统管理/系统配置/日志中心配置/外置日志中心]项“关闭内置日志中心，以减少设备的资源消耗，提高日志记录性能”。

终端安全

1. 僵尸主机检测

深信服僵尸主机检测，通过僵尸网络行为分析和特征识别相结合，可识别并阻断内网安全域中疑似中了病毒木马的僵尸主机，内置的云安全检测技术，针对未知可疑风险上报云端虚拟沙盒执行并下发分析结果报告，有效防止主机访问非法恶意链接导致中招。

勾选“启用僵尸网络检测”，开启功能。

排除IP：不需要检测的IP，可以加入白名单。

排除网站：不需要检测的网站，可以加入白名单。

处理动作：可以选择告警通知（需要配合系统管理-系统配置-告警选项使用）、阻断恶意连接或冻结源IP。

2. 终端监测与响应（EDR）

深信服EDR作为终端检测响应平台，轻量级终端+管理平台组成的解决方案，利用对终端威胁的持续检测能力，对威胁事件进行一键隔离的响应设置，深信服的EDR产品与NGAF、AC、SIP产品的联动协同响应，形成新一代的安全防护体系。此功能适用于已部署本地EDR或SaaS-EDR产品，AC支持和本地EDR或SaaS-EDR联动。

操作步骤

• 本地部署EDR联动

步骤1.在EDR管理平台的[系统设置/系统管理/基本设置]中打开联动设备准入的开关。

说明

如果EDR设备未勾选联动设备准入设置，在AC设备上填写接入IP设置时会提示“自动密码协商失败，请稍后重试”。

步骤2.在AC设备的[安全管理/终端上网安全/安全配置/终端检测与响应（EDR）]中选择本地接入，填入本地EDR管理IP，点击<接入>。

步骤3.联动成功后显示EDR服务信息、接入EDR终端数和已联动处置次数。

步骤4.点击<查看联动详情>，跳转到联动终端详情页面。

序号	联动终端	联动终端IP	状态	联动操作数	最近更新时间	...
1	DESKTOP-77USOGL	172.16.1.250	离线	0	2023-07-25 10:26:08	

说明

上述步骤完成AC和本地EDR的联动，联动完成后可配置AC和EDR的联动动作，下面举例AC联动EDR推送EDR agent。

步骤5.推送EDR agent设置。点击右上角<推送配置>会跳转到EDR推送配置页面，该功能默认关闭，勾选“启用推送配置”，配置相关参数。

策略适用范围：配置需要推送EDR客户端的内网IP或者IP段。对适用范围内的终端推送EDR客户端部署通知的web页面，帮助内网推送EDR的终端。

是否强制重定向：勾选强制重定向后“推送时间间隔”将会失效，未安装EDR终端将始终重定向到EDR agent下载页面。

重定向地址：填写EDR agent下载页面。获取方法：在EDR设备的[系统管理/终端部署/网页推广部署]获取部署时的web页面链接。重定向会推送安装页面导致断网，请挑选业务可终端时间开启。

推送时间间隔（s）：定义多长时间向未安装agent的客户端推送一次页面，默认300s。

效果展示：

适用策略地址范围的终端，没有安装EDR时，打开浏览器访问网站会重定向到深信服EDR终端防护中心部署通知页面，页面提供Window、Linux两种操作系统的方式。

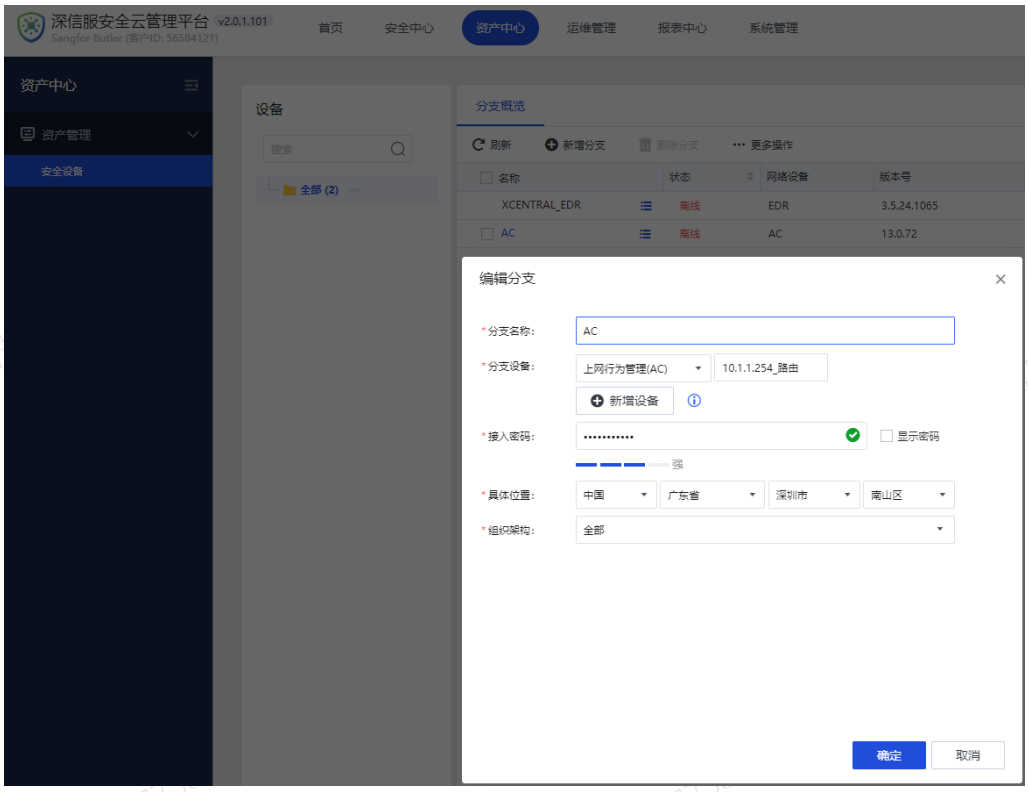
此时，客户端根据提示，下载对应操作系统的安装包，完成安装。

说明

支持对http/https网页重定向。内网所有用户完成EDR agent安装后，可根据需求关闭推送EDR agent设置。

- **SaaS-EDR联动**

步骤1.AC和SaaS-EDR联动时，AC需要加入和SaaS-EDR同一云图平台。在[资产中心/资产管理/安全设备]中新增分支AC。



步骤2.在SaaS-EDR管理平台的[系统设置/系统管理/基本设置]中打开联动设备准入的开关。

步骤3.在AC设备的[安全管理/终端上网安全/安全配置/终端检测与响应（EDR）]中选择云端接入，填写云图的企业ID、接入设备名称、接入密码，其中接入设备名称、接入密码和云图上新建分支AC时所配置的参数保持一致。

步骤4.联动成功后显示EDR服务信息、接入EDR终端数和已联动处置次数。

步骤5.点击<查看联动详情>，跳转到联动终端详情页面

说明

上述步骤完成AC和SaaS-EDR的联动，联动完成后可配置AC和EDR的联动动作，下面举例AC联动SaaS-EDR推送agent。

步骤6.推送SaaS-EDR agent配置。点击右上角<推送配置>会跳转到EDR推送配置页面，该功能默认关闭，勾选“启用推送配置”，配置相关参数。

策略适用范围：配置需要推送EDR客户端的内网IP或者IP段。对适用范围内的终端推送EDR客户端部署通知的web页面，帮助内网推送EDR终端。

是否强制重定向：勾选强制重定向后“推送时间间隔”将会失效，未安装EDR终端将始终重定向到SaaS-EDR agent下载页面。

重定向地址：填写SaaS-EDR agent下载页面。获取方法：在云图平台SaaS-EDR[系统管理/终端部署/网页推广部署]获取部署时的web页面链接。重定向会推送安装页面导致断网，请挑选业务可终端时间开启。

推送时间间隔（s）：定义多长时间向未安装agent的客户端推送一次页面，默认300s。

效果展示：

适用策略地址范围的终端，终端未安装SaaS-EDR agent时，打开浏览器访问网站会重定向到深信服SaaS-EDR终端防护中心部署通知页面，页面提供Window、Linux两种操作系统的方式。

此时，客户端根据提示，下载对应操作系统的安装包，完成安装。

注意事项：

1. AC和SaaS-EDR联动时需要加入云图，由于AC集中管理只能加入BBC或云图，所以已加入BBC的AC设备需要解除集中管理再加入云图，即已部署BBC场景不适用于和SaaS-EDR联动。
2. AC和SaaS-EDR联动时，由于SaaS-EDR部署在互联网，终端重定向的SaaS-EDR终端防护中心部署通知页面，以及SaaS-EDR agent下载链接都处于互联网，AC需要把这些域名加入全局排除地址，如互联网出口有网络安全设备，也需要同步放行（edrsaas.sangfor.com.cn、dledragent.sangfor.com.cn、edragent.sangfor.com.cn、download.sangfor.com.cn、edrinterco
3. SaaS-EDR终端防护中心部署通知页面链接有效期是60天，如果需要长时间推送SaaS-EDR agent，需要在EDR推送配置定时刷新重定向地址。
4. 云图EDR未授权，不能接入，已授权且在有效期内才能正常接入。

3. 补丁检测

Windows补丁检测功能，能够及时检测客户端计算机当前未安装的补丁和补丁更新提示，能够使安全意识不足的用户主动提高操作系统安全性，帮助管理员减少来自内网安全方面的工作压力。

点击<去设置补丁包检测>跳转到[接入管理/接入认证/检查规则/终端插件检查规则]页面，详细配置请参考终端检查案例。

网络安全

1. 防内网DOS攻击

DOS攻击（拒绝服务攻击），通常是以消耗服务器端资源、迫使服务停止响应为目标，通过伪造超过服务器处理能力的请求数据造成服务器响应阻塞，从而使正常的用户请求得不到应答，以实现其攻击目的。SANGFOR设备的防内网DOS攻击功能，也可以阻止内网的机器中毒或使用攻击工具发起的DOS攻击。AC的内网DOS攻击功能，只关注LAN口方向。

防内网DOS攻击有三种检测方式：SYN泛洪、UDP泛洪、ICMP泛洪。

SYN泛洪：攻击者发送TCP SYN，SYN是TCP三次握手中的第一个数据包，而当服务器返回ACK后，该攻击者就不对其进行再确认，那这个TCP连接就处于挂起状态，也就是所谓的半连接状态，服务器收不到再确认的话，还会重复发送ACK给攻击者。这样更加会浪费服务器的资源。攻击者就对服务器发送非常大量的这种TCP连接，由于每一个都没法完成三次握手，所以在服务器上，这些TCP连接会因为挂起状态而消耗CPU和内存，最后服务器可能死机，就无法为正常用户提供服务了。

UDP泛洪：攻击者发送大量的UDP包给服务器，服务器发送大量回复。

ICMP泛洪：攻击者发送数据包的源IP地址是被攻击者的IP地址，目的IP地址是被攻击者所在网段的广播地址，这样大量ICMP echo reply就到了被攻击者那里。

以下IP地址发起的攻击不会被拦截：对填入列表中的IP地址不进行DOS防御，比如内网有一台向公网提供服务的服务器，并且提供给公网的连接较多，此时建议将服务器的地址排除，避免被DOS防御认为是非法的。

点击<配置>，启用内网网段列表，可配置通过设备上网的内网网段，不在列表的用户默认为攻击用户。启用后不在列表内的用户数据无论是否被攻击会被拦截。

防内网DOS攻击处理动作可选择：告警通知、封锁攻击、推送EDR。

- **告警通知：是启用事件邮件告警功能，详细配置请参考告警选项章节。**
- **封锁攻击：设置设备在检测到攻击以后对主机的封锁时间。**
- **推送EDR：勾选推送EDR需先开启终端检测与响应的推送配置。**

点击<提交>，用于保存配置。

2. 防ARP欺骗

ARP欺骗是一种常见的内网病毒，中病毒的电脑，不定时地向内网发ARP欺骗的广播包，使内网机器的正常通信受到干扰和破坏，严重时会导致断网。

设备的防ARP欺骗是通过设备和内网PC的准入客户端配合来实现的。

设备通过不接受有攻击特征的ARP请求或回复来保护设备本身的ARP缓存，实现自身的免疫。

如果设备的访问控制用户有绑定IP/MAC，则设备会以绑定的IP/MAC信息为准。

内网PC的防ARP欺骗是通过准入客户端来实现的。安装了准入客户端后，准入客户端会和设备通讯，获取设备和网关的正确IP/MAC关系并静态绑定。

启用ARP欺骗防护：是启用ARP欺骗防护的总开关。

启用静态ARP：如果内网PC的网关不是设备的接口地址，那就需要在这里设置，比如设备使用网桥模式，内网PC的网关地址应该是前面的路由器（或防火墙）接口地址，这时我们就可以把前面路由器的接口IP/MAC填入下面的方框里。内网PC如果安装了准入客户端就可以获取正确的网关IP/MAC并进行绑定，这样可以保证PC机上网关的IP/MAC是正确的，保证PC和网关的正常通信。

设定网关MAC广播间隔时间（秒/次）：是设置广播网关（即设备的内网接口）MAC的时间间隔，建议设成10秒。

处理动作可勾选告警通知，启用事件邮件告警功能，详细配置请参考告警选项章节。

点击<提交>，用于保存配置。

3. 恶意链接

结合深信服云引擎，综合多重恶意软件检测机制，利用静态检测、动态沙箱、污点跟踪、人工分析等技术进行综合判定，实时识别恶意链接，保障用户业务免受影响，包括钓鱼及恶意网站、漏洞利用、挖矿页面、恶意跳转、跨站脚本攻击和病毒文件等。

勾选“启用恶意链接检测”，开启功能。

排除IP：不需要检测的IP，可以加入白名单。

排除网站：不需要检测的网站，可以加入白名单。

处理动作：可以选择告警通知详细配置请参考告警选项章节、阻断恶意链接方式。

4. SAVE杀毒

SAVE（Sangfor AI-based Vanguard Engine）结合深度学习等多种机器学习算法，使用集成学习充分利用各个算法的检测优势，能快速、准确捕捉文件的有效信息，对勒索病毒的检出率达到业界领先水平。通过安全云脑、EDR和AF等产品持续汇聚热门威胁的分析，SAVE安全智能检测引擎能够及时演进，从而提升检测能力，并覆盖最新的病毒。

SAVE杀毒主要用于对经过设备的数据进行病毒查杀，保护内网计算机的安全。设备能针对HTTP、FTP、POP3、SMTP这四种常用协议进行查杀病毒。设备中内置了深信服自主开发的SAVE引擎，具有病毒识别率高和查杀效率高的特点。SAVE引擎不同于传统的规则库更新，为了保持习惯，是以规则库的形式显示，更新周期是2个月。

SAVE杀毒配置界面四种协议杀毒的开关、不需杀毒的网站或文件白名单。

管理员可根据需求启用HTTPS下载杀毒、HTTPS下载杀毒、启用FTP下载杀毒、启用POP3/ICMP杀毒，启用SMTP杀毒。

其中HTTPS下载杀毒和POP3和IMCP杀毒、SMTP功能需要配合启用访问权限策略中的SSL内容识别和邮件过滤功能。

启用排除网站（域名）：可设置访问特殊网站的数据不需要杀毒，输入格式为域名格式，支持通配符，一行一个域名。

启用文件白名单：用于定义不需要杀毒的文件。

扫描文件格式：用于定义需要进行SAVE扫描文件的后缀。

扫描文件大小：用于定义需要进行SAVE扫描文件的大小。

处理动作：勾选告警通知时需要配合[系统管理/系统配置/告警选项]，详细配置请参考告警选项章节。

点击<病毒库升级>，会显示升级服务有效期和当前SAVE引擎模型日期。

[从本地加载SAVE引擎模型升级]：用于将下载好的SAVE引擎模型文件手动导入到设备中并完成SAVE引擎模型的升级，点击<选择文件>选择要导入的SAVE引擎模型文件，完成SAVE引擎模型的升级。

安全状态

此章节与[全网监控/安全状态]章节内容均一致，点击安全状态可跳转到该章节。

终端提醒策略

终端提醒策略是对用户的上网行为进行提醒的功能，管理员可以通过配置终端提醒策略来对上网用户推送公告页面，此功能是通过定期把HTTP流量重定向到指定的公告页面，从而把公告信息通过浏览器传送到终端用户。

操作步骤

步骤1.在[安全管理/终端提醒策略]，点击<新增>选择终端提醒策略。

步骤2.勾选启用该策略，并填写策略名称和策略信息，策略名称是策略的唯一标识，不能重复且为必填项，描述信息是对策略的概要描述，非必填项。

步骤3.点击<策略配置>进入策略设置页面，勾选公告页面，进行相应的终端提醒策略的设置。

提醒频率：可选择每隔一段时间进行公告页面的推送，或者定时推送。

每隔（分钟）：设置时间间隔，范围是1-1440。

定时： 在设定的时间点，推送公告页面。

公告页面选择（需要确保中能用户能正常访问到该页面）

• 使用设备内置的公告页面：设置里面的内置公告内容的具体设置需要到[系统管理/系统配置/终端提示页面定制]，请参考终端提示页面定制章节。

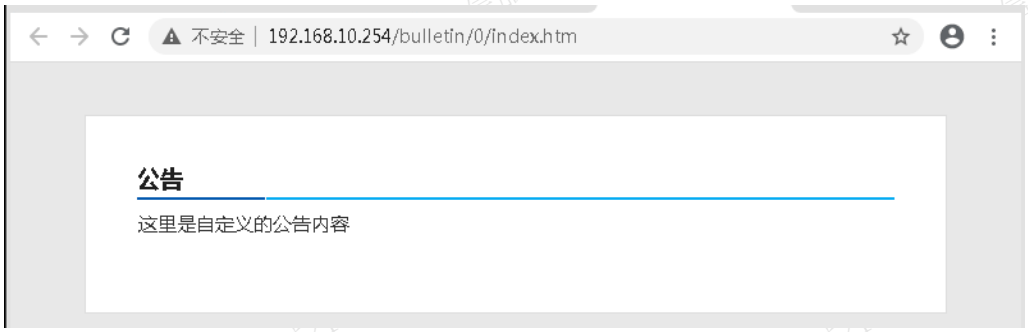
• 使用外部的公告页面：在[URL]中设置自定义页面的URL，可以直接以URL的方式链接到您所需要的公告页面。

步骤4.点击<适用对象>来配置适用组和用户，此处选中的用户组和用户将全面匹配此终端提醒策略。

步骤5.点击<高级配置>，可配置策略过期日期设置、同级别管理员查看编辑权限设置和是否允许低级别管理员查看。

步骤6.点击<提交>，完成配置。

步骤7.当用户在设置提醒频率的时间间隔访问HTTP网站时，会出现该提示页面。



终端安全联动

终端安全联动是针对深信服各安全产品通过联动码完成相互间联动的功能。AC可与ZTA平台建立联动，实现从ZTA平台同步用户信息，完成单点登录；并支持AC上报业务审计和文件审计日志到ZTA平台。AC可与终端安全管理系统EDR、零信任访问控制系统aTrust建立联动，提供统一客户端安装、统一系统托盘、产品功能联动等特性。

ZTA平台对接

实现效果

1. 同步ZTA用户信息：AC从ZTA平台同步用户上线/下线信息，完成单点登录，用户信息和审计日志关联，利于溯源分析。
2. 日志同步：AC将业务审计和文件审计日志转发到ZTA平台，利于ZTA平台对日志统一分析。

功能配置

步骤1.在[安全管理/终端安全联动]选择<生成联动码>，选择本设备IP地址，该地址用于和ZTA平台对接，并填入联动设备名称和备注，点击<立即生成>可生成设备联动码。

步骤2.在ZTA平台[系统/组件管理/深信服联动设备]添加接入联动设备，填入AC生成的设备联动码，完成AC

和ZTA平台联动。并在AC中可查看联动状态。

步骤3.在AC[接入管理/接入认证/PORTAL认证/认证策略]新增认证策略，认证范围填入需要和ZTA单点登录的地址范围，认证方式选择单点登录，认证后处理根据实际需求选择是否自动录入用户到本地 组织结构和自动录入绑定关系。

步骤4.在AC[行为审计/业务审计策略]新增业务审计策略，对Web、SMB、FTP业务系统开启审计。

步骤5.在AC[行为审计/上网审计策略]新增上网审计策略，对Web邮箱、论坛、微博等网页文件外发进行审计（https网页需要开启解密）。

步骤6.在AC[行为审计/客户端审计策略]新增客户端审计策略，对IM、邮件、网盘等应用外发文件进行审计（需要安装准入客户端）。

步骤7.进入AC内置日志中心[系统管理/日志导出/服务器配置]，在深信服对接上报中启用ZTA日志上报功能，并填入ZTA分析平台地址。

注意事项

1. AC的系统时间需要和ZTA的系统时间一致，不然会造成日志错乱。
2. AC暂时不支持高可用。
3. AC同步用户只支持小写用户名，不支持用户名包含大写字母，如ZTA用户包含大写字母，同步到AC时会自动转为小写（如果配置了用户信息同步和日志同步，ZTA包含大写字母的用户同步到AC后转换为小写，AC再同步日志到ZTA平台时，ZTA平台搜索不到该用户，造成日志信息不匹配）。
4. AC需要关闭无流量注销，否则会造成用户被下线。
5. 外置日志中心不支持ZTA上报日志。
6. 海外IAG不支持ZTA对接。
7. 内置日志中心启用ZTA日志上报功能，同时会自动关闭syslog、ftp服务器配置导出。
8. 因为AC日志中心形成日志文件的时间间隔为5分钟，在日志上报过程中，如果AC从ZTA1平台切换到ZTA2平台，ZTA1会丢失1~5分钟的日志，ZTA2不受影响。如在第3分钟AC从ZTA1切换到ZTA2，那么第0-3分钟的日志不会上报到ZTA1，而是等到第5分钟后全部上报到ZTA2，即ZTA1会丢失第0-3分钟的日志。

9. 启用ZTA日志上报功能，无法使用FTP、syslog日志导出。

终端All in one

AC+EDR配置案例

需求背景

随着企业在终端安全侧的投入越来越大，针对不同的安全需求部署不同的安全策略，以往传统的终端安全策略每个独立的产品需要安装独立的客户端，多个客户端对终端PC的资源消耗，终端兼容性问题以及终端管理问题日益突出，企业需要具备端点、网络、应用程序工作负载、数据、通信、以及用户工作负载访问控制高度集成的一体化端点安全安全办公解决方案。

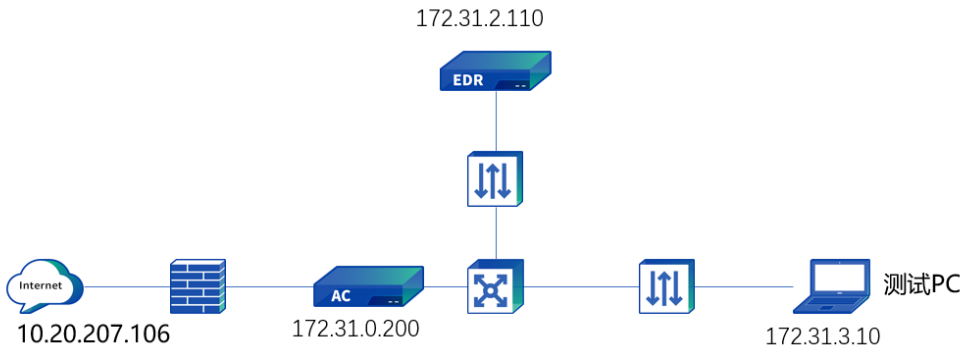
方案介绍

深信服终端All in one（以下简称AIO）针对深信服各安全产品，提供统一客户端安装、统一系统托盘、产品功能联动等特性，结合EDR的全面部署应用，提供全网终端病毒、木马、入侵攻击等威胁防御能力，提供行之有效的整体安全防御体系，办公安全一端足矣

实现效果

1. **统一安装：**管理员通过配置客户端集成规避了重复推端，用户只需要安装一次就可以安装完所需安装的深信服客户端（EDR、AC），简化了管理员的客户端推广工作，简化了用户的安装体验，并在一定程度上减少投诉。
2. **统一系统托盘：**用户可以通过统一的深信服产品托盘进入不同产品界面，在一定程度上降低用户对多客户端托盘的排斥，在一定程度上减少用户的抱怨与投诉，补齐在与友商竞争中一体化客户端的短板。

部署方案



1. AC网桥模式部署在互联网出口，针对内网用户开启准入功能。
2. EDR管理平台（172.31.2.110）部署在运维区，用户可直接通过EDR管理平台获取EDR客户端完成安装。

产品线	版本	备注
EDR	3.7.10	
AC	13.0.102	

说明：

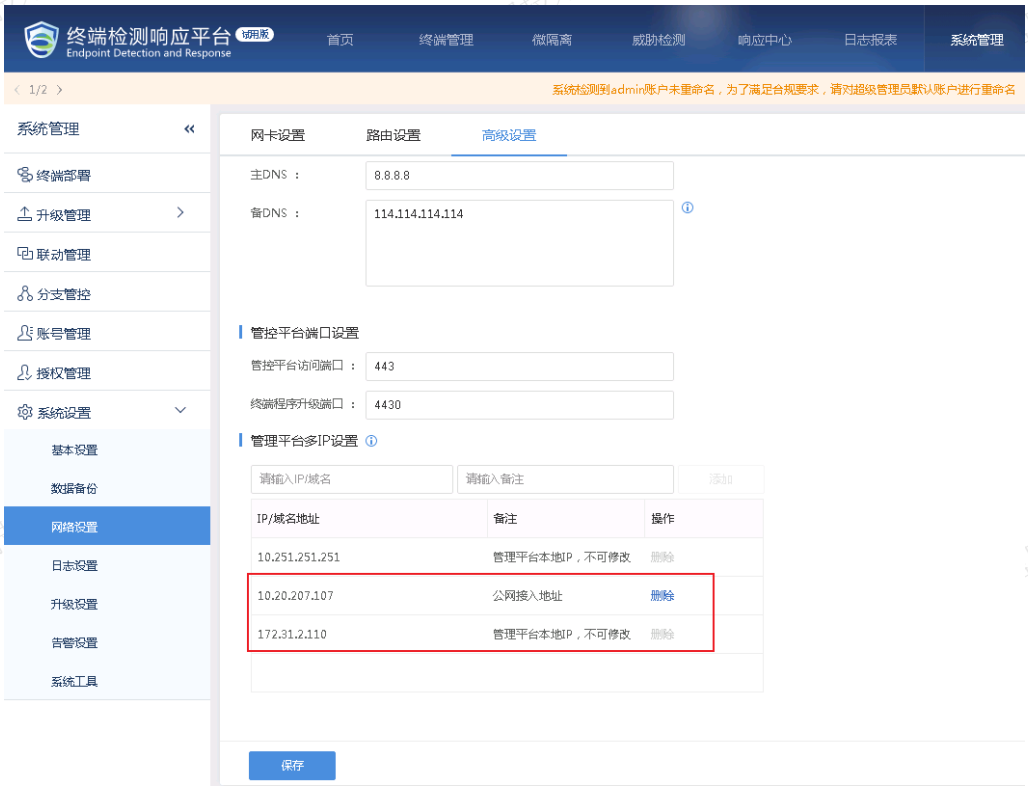
AC联动通信端口为AC开放接口端口TCP9998，aTrust控制器、EDR管理平台的联动端口均为TCP443，内网如果有防火墙之类的安全设备，需要放通联动端口。

功能配置

设备对接配置

步骤1.在[系统管理/系统设置/网络设置/高级配置/管理平台端口设置]页面，可以修改EDR管理平台控制台端口和终端程序升级安装端口。

步骤2.需要在EDR[管理平台多IP设置]页面，将客户端下载的地址配置进来，如果EDR有多个IP，或者用户通过公网接入，需要将用户可以下载的IP地址，以及前置网关映射的公网IP地址都填入进来。



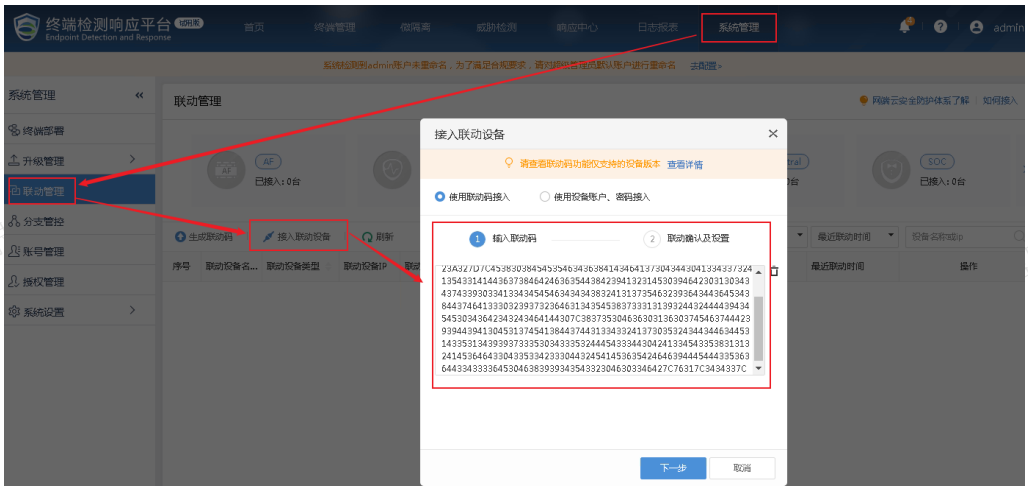
说明：

联动规则是读取EDR的这两处配置，生成客户端下载安装地址，下发给客户端。

步骤3.登陆AC控制台，在[安全管理/终端安全联动]页面，选择跟联动设备通信的IP地址后，点击生成联动

授权码。

步骤4.在EDR管理端[系统管理/联动管理]页面，点击接入联动设备，粘贴AC上生成的联动码，点击<下一步>后可以读取到AC的连接信息，选择与AC通信的IP地址后点击确定即可。



步骤5.配置完成后，点击【连通性测试】测试联动配置是否成功。

步骤6.通过AC也可以看到EDR联动状态已经成功。

说明

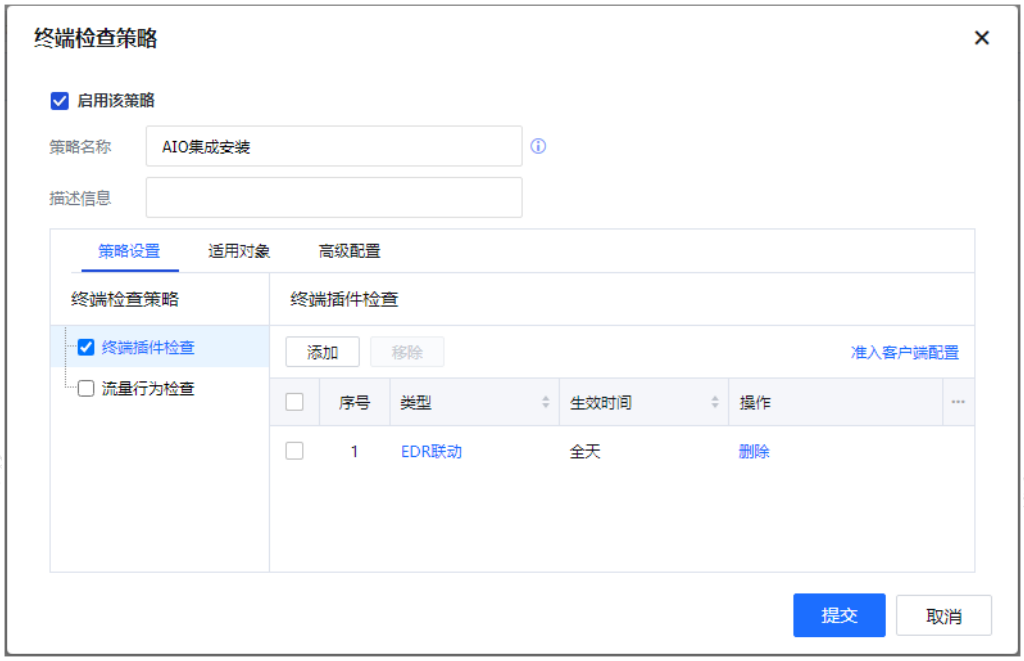
：

也可以在EDR生成联动码，在AC识别联动码生成关联关系。

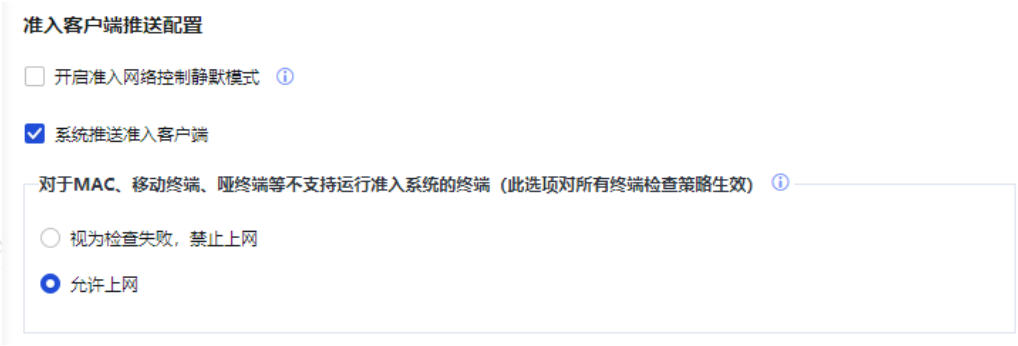
启用集成策略

步骤1.在AC控制台[接入管理/终端管理/终端检查规则/插件检查规则]页面，新增[客户端集成规则]，输入规则名称、规则类型、规则描述，客户端需要集成的设备选择配置的联动的EDR设备。

步骤2.在AC[接入管理/终端管理/终端检查策略]新增检查策略，将创建的集成策略关联给需要安装AIO客户端的用户。



步骤3.在AC[接入管理/终端管理/准入客户端配置]页面开启准入推送策略



说明

：

准入策略启用后，目标终端会显示准入安装页面，上网过程会中断直至准入安装完毕，建议开启策略前提前通知用户。

步骤4.用户如果需要通过先安装EDR再联动安装AC客户端，还需在[系统管理/系统设置/基本设置]页面勾选[客户端集成并下载AC零信任客户端]选项。

说明

：

1.如果所有用户均通过先安装AC准入客户端再联动下载EDR客户端，也可不开启该选项。

2.以EDR为起点联动推送安装AC和aTrust为全局推送，不支持指定用户推送。

客户端使用

• 客户端安装

1. 全新安装场景(客户当前无AC准入和EDR)，该场景面向用户新上AC准入和EDR场景。

步骤1.AC开启准入策略后，用户上网流量经过AC，AC会重定向用户至安装准入客户端页面。

步骤2.下载安装完成后，如果未开启准入认证客户端，可在任务管理器看到准入进程。

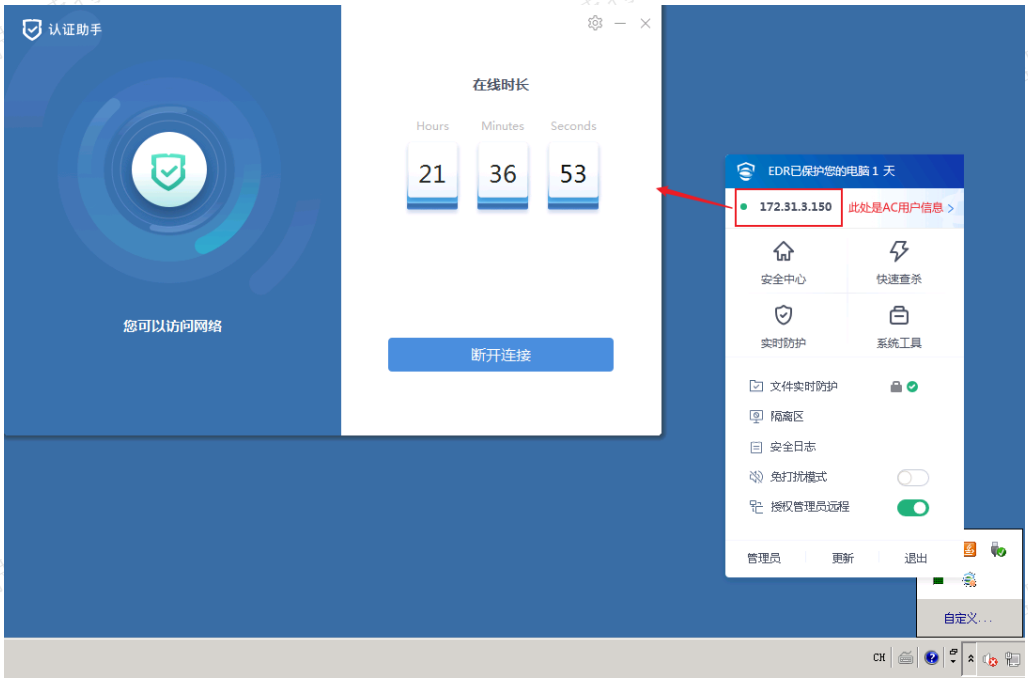
步骤3.用户关联了集成安装策略，EDR客户端会在后台静默下载安装（由于EDR安装包比较大，内网环境需要等待5-10分钟）。

说明：

当前版本EDR后台安装暂时没有下载和安装进度可以展示。

步骤4.等待EDR客户端安装完成后，如果用户未开启AC准入认证，系统托盘只有EDR客户端。

步骤5.如果用户开启了AC准入认证客户端，系统托盘会展示AIO融合后的图标。

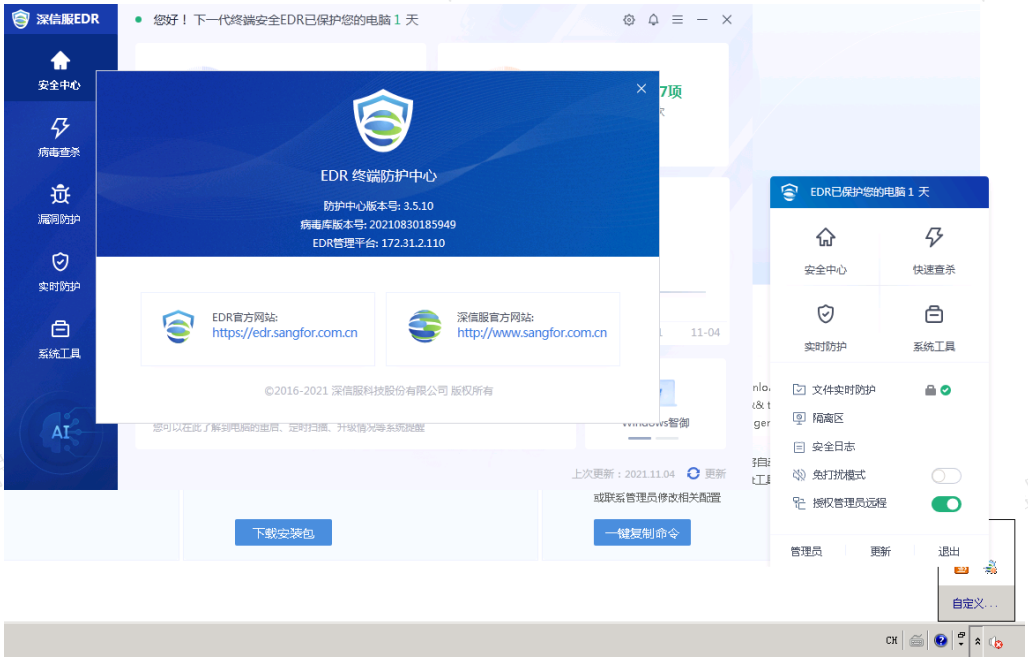


说明

：

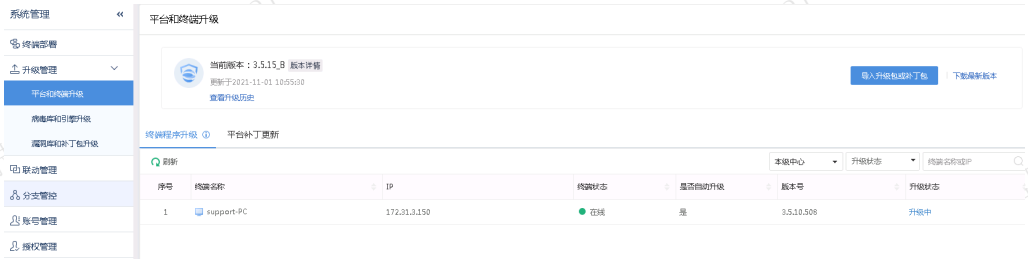
AC+EDR场景下，AIO系统托盘主界面为EDR客户端。

2. 升级场景(客户当前有AC和EDR客户端)，该场景面向已经部署过老版本AC和EDR客户端的用户。



步骤1.首先需要升级AC和EDR至AIO版本，具体升级过程请参考各产品线升级操作指导。

步骤2.设备升级完成后，AC准入客户端和EDR均会静默升级，可通过EDR管理平台查看终端升级状态，升级完成后，系统图标会融合成一个。



说明：

由于EDR客户端升级包比较大，内网环境下升级预计5-10分钟，升级过程需要耐心等待。

3. 加装场景(客户当前有AC，但是没有EDR)，该场景面向已经部署AC准入客户端，新增部署EDR客户端的用户。

步骤1.用户如果部署的AC为非AIO版本，需要先完成AC设备升级，并完成EDR设备部署和联动配置，具体各项配置与前述基本一致。

步骤2.客户端AC准入找到网关后，客户端会静默升级，升级完成后会在后台静默安装EDR客户端，EDR静默安装过程需要耐心等待。

步骤3.客户端升级安装全部完成后，客户端系统托盘会融合成一个，具体过程与新装和升级场景基本一致。

4. 加装场景(客户当前有EDR，但是没有AC)，该场景面向已经部署EDR客户端，新增部署AC准入客户端的用户。

步骤1.用户如果部署的EDR为非AIO本，需要先完成EDR管理平台升级，并完成AC设备部署和联动配置，各项配置与前述基本一致。

步骤2.EDR平台升级完成以后，客户端会自动静默升级，升级过程需要耐心等待。

步骤3.EDR管理平台如果同步开启了【客户端集成并下载AC准入客户端】选项，客户端更新成功后会自动在后台静默安装AC准入客户端。

步骤4.客户端升级安装全部完成后，客户端系统托盘会融合成一个，具体过程与新装和升级场景基本一致。

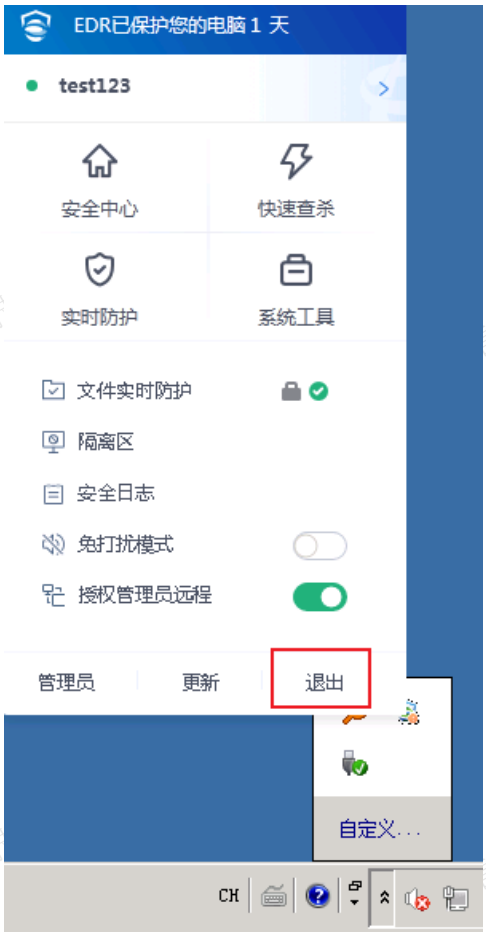
- 客户端使用

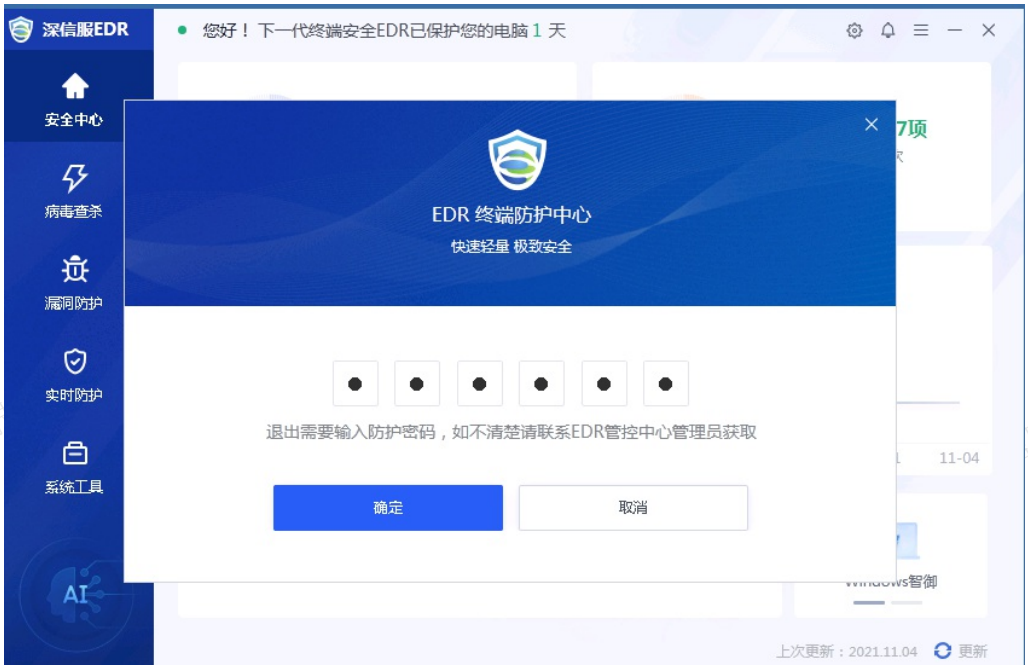
1. 当EDR与AC集成时，当AC开启准入认证策略，并且终端用户未认证前，托盘上方显示“上网认证”的按钮。

2. 用户如果已经认证在线，则看到的是用户认证信息。

• 客户端退出

步骤1.AC和EDR无法一次性整体退出，右键点击系统托盘，点击退出选项，输入EDR退出密码，退出的是EDR的单独客户端。

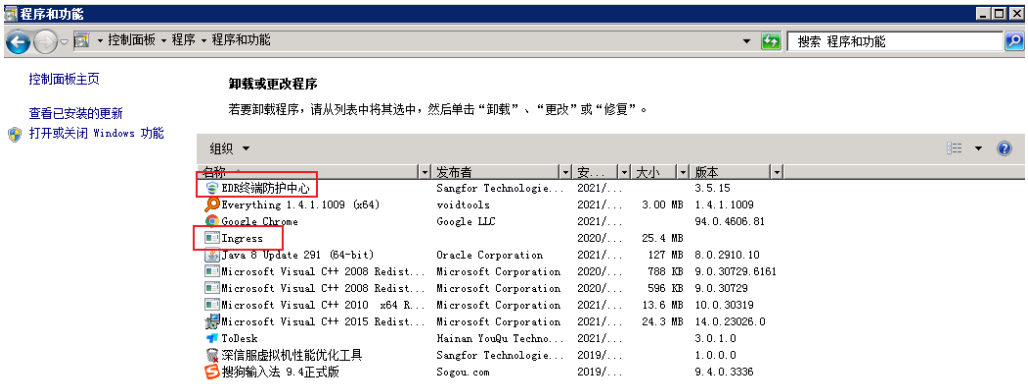




步骤2.EDR客户端退出后，系统托盘将变为独立的AC认证客户端托盘，如需整体退出，还需要单独再次退出AC的认证客户端，AC认证客户端退出后，用户会注销下线。

• **客户端卸载**

当前版本各产品线卸载相互独立，互不干扰。



注意事项

1. AIOv3.0版本当前仅支持windows PC版本中文操作系统，暂不支持MAC、linux以及windows server版操作系统。

产品线	Win XP	Win 7	Win 8	Win 8.1	Win 10	Win 11
EDR	Y	Y	Y	Y	Y	Y
AC	N	Y	Y	Y	Y	Y
aTrust	N	Y	N	N	Y	Y

2. 用户如果手动卸载客户端以后，注册表会保留已安装过的标记，重新安装任意客户端AIO将不再联动下载安装其他客户端，避免用户手动卸载后重复推送，如果用户想重新安装其他客户端，也需要手动下载安装（如需恢复联动下载，可在注册表删除软件安装标识HKEY_LOCAL_MACHINE\SOFTWARE）。
3. AC主主、主备模式场景下，因为联动ID集群模式为一个，当主节点异常使得另一台节点工作并以新节点管理IP+联动ID与EDR或atrust建立互信时，因为管理IP变化会被拒绝，因此当前版本暂不建议在AC高可用环境下使用AIO集成安装策略。
4. EDR PC基础版的授权不支持AIO联动，其他PC高级版、全量版、服务器旗舰版、全量版均支持AIO，探针版也支持AIO，不过探针版没有托盘统一。

AC+EDR+aTrust配置案例

需求背景

随着企业在终端安全侧的投入越来越大，针对不同的安全需求部署不同的安全策略，以往传统的终端安全策略每个独立的产品需要安装独立的客户端，多个客户端对终端PC的资源消耗，终端兼容性问题以及终端管理问题日益突出，企业需要具备端点、网络、应用程序工作负载、数据、通信、以及用户工作负载访问控制高度集成的一体化端点安全办公解决方案

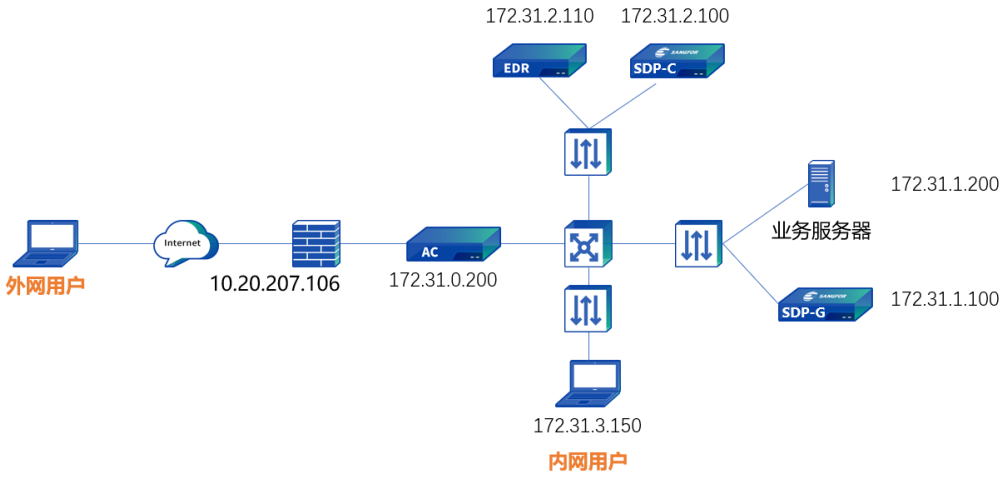
方案介绍

深信服终端All in one（以下简称AIO）针对深信服各安全产品，提供统一客户端安装、统一系统托盘、产品功能联动等特性，结合EDR的全面部署应用，提供全网终端病毒、木马、入侵攻击等威胁防御能力，提供行之有效的整体安全防御体系，结合零信任安全办公，在终端与接入建立控制点，为客户提供内网办公、远程办公、混合办公一体化的整体解决方案，办公安全一端足矣。

实现效果

1. **统一安装：**管理员通过配置客户端集成规避了重复推端，用户只需要安装1次就可以安装完所需安装的深信服客户端（aTrust、EDR、AC），简化了管理员的客户端推广工作，简化了用户的安装体验，并在一定程度上减少投诉。
2. **统一系统托盘：**用户可以通过统一的深信服产品托盘进入不同产品界面，在一定程度上降低用户对多客户端托盘的排斥，在一定程度上减少用户的抱怨与投诉，补齐在与友商竞争中一体化客户端的短板。
3. **统一客户端工作台：**围绕安全办公场景，atrust提供客户端工作台，可在工作台上进行认证登录和访问资源；并在工作台融合EDR、AC功能访问入口，在工作台安全页面进行EDR客户端功能快捷操作和状态集成。
4. **EDR和aTrust联动：**通过EDR对终端环境进行检测，当存在风险时，禁止用户通过不安全终端访问业务，隔离来自终端的风险。

部署环境



1. *SDP采用控制器+代理网关的部署架构，控制器（172.31.2.100）部署在运维区，代理网关（172.31.1.100）部署在业务区。*
2. *AC网桥模式部署在互联网出口，针对内网用户开启准入认证功能。*
3. *EDR管理平台（172.31.2.110）部署在运维区，用户可直接通过EDR管理平台获取EDR客户端完成安装。*
4. 互联网出口防火墙对外发布aTrust、AC和EDR管理平台相关服务。
5. 用户内外网访问业务系统均通过aTrust代理访问，保持业务访问体验一致性。

产品线	版本	备注

EDR	3.7.10	
aTrust	2216	
AC	13.0.102	

说明：

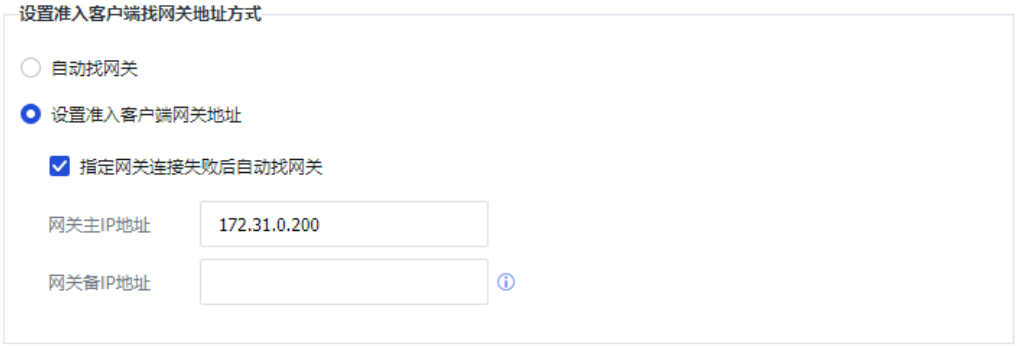
AC联动通信端口为AC开放接口端口TCP9998，aTrust控制器、EDR管理平台的联动端口均为TCP443，内网如果有防火墙之类的安全设备，需要放通联动端口。

功能配置

AC、EDR、aTrust基础网络部署请参考安装部署手册，以下配置为终端All in one联动相关配置。

接入配置

步骤1.登录AC管理页面，在[接入管理/终端管理/准入客户端配置]页面修改准入找网关方式为指定地址，即选择[设置准入客户端网关地址]，并配置网关主、备IP地址。



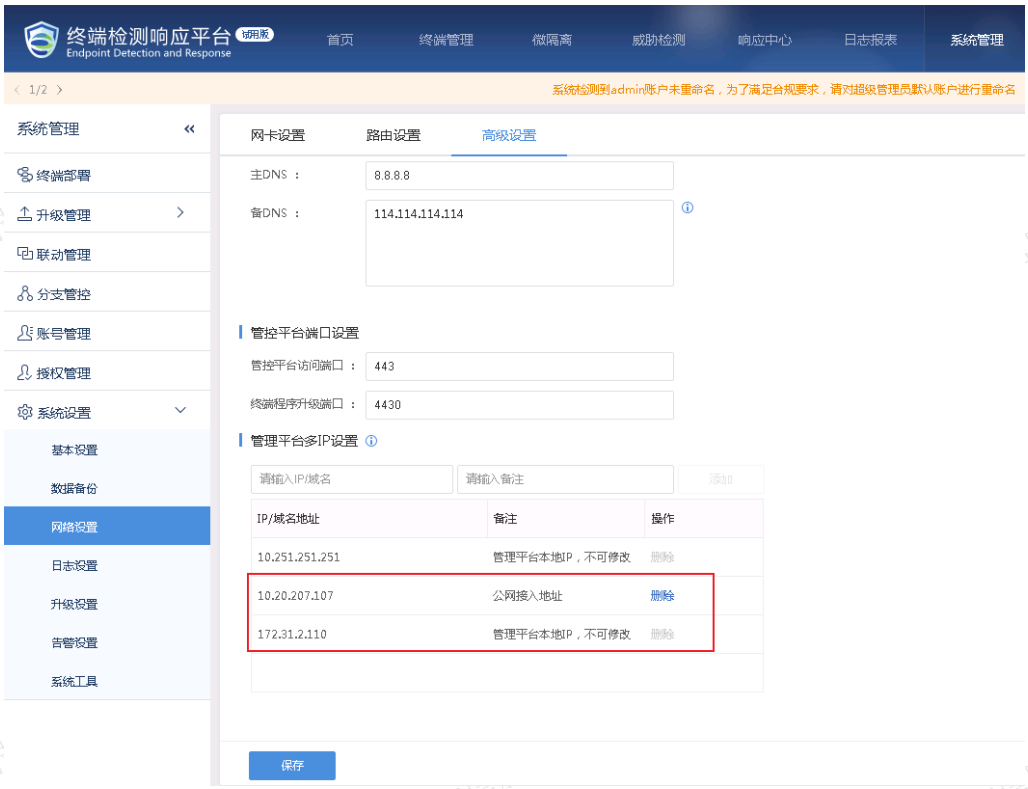
说明：

1.联动规则读取的是该地址推送给终端进行联动下载AC准入客户端，因此需要务必确保测试PC能够与设置的IP地址正常通信，具体通信端口详见4.3章节服务端口清单。

2.该地址需要在配置集成安装策略前完成配置，如果配置完集成安装策略在再修改该地址，需要先关闭再重开集成策略触发更新，例如，在aTrust集成安装AC准入客户端时，需要在aTrust全局/用户策略把集成AC的选项的勾关闭，再打开进行触发更新。

步骤2.登录EDR管理平台，在[系统管理/系统设置/网络设置/高级配置/管理平台端口设置]页面，可以修改EDR管理平台控制台端口和终端程序升级安装端口。

步骤3.需要在[管理平台多IP设置]页面，将客户端下载的地址配置进来，如果EDR有多个IP，或者用户通过公网接入，需要将用户可以下载的IP地址，以及前置网关映射的公网IP地址都填入进来。

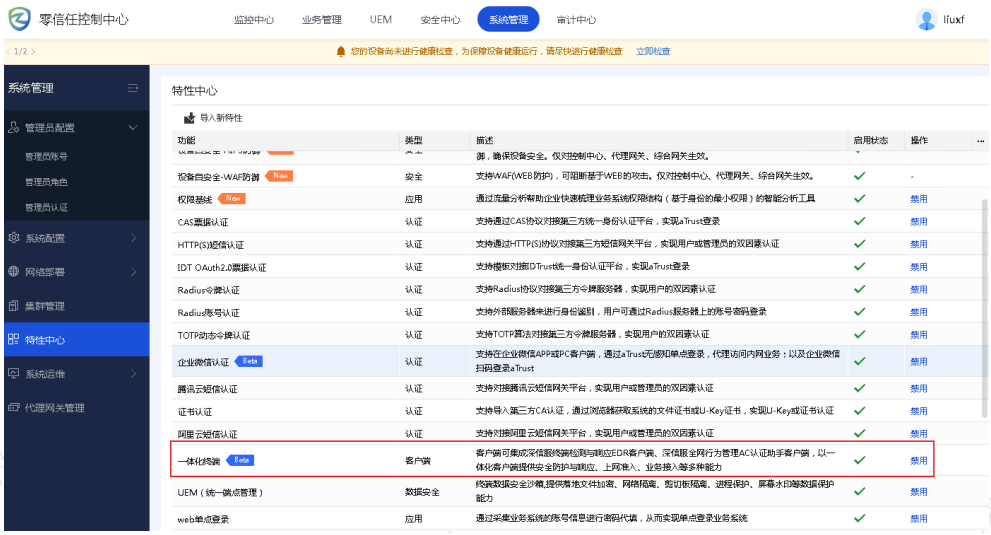


说明：

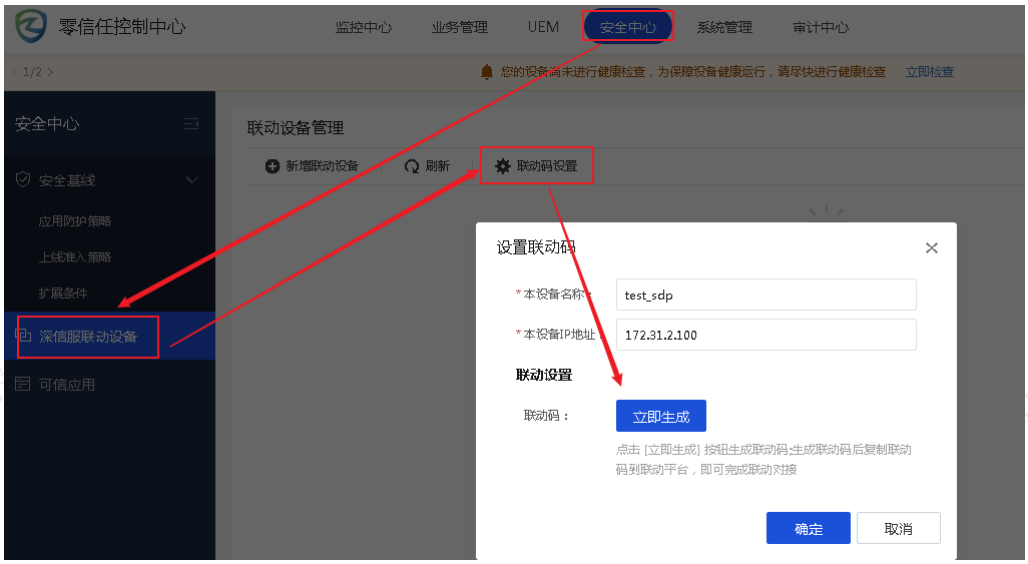
联动规则是读取EDR的这两处配置，生成客户端下载安装地址，下发给客户端。

联动码配置

步骤1.登陆aTrust管理端，在[系统管理/特性中心]，开启[一体化终端]特性。



步骤2.在aTrust管理端[安全中心/深信服联动设备]页面，点击[联动码设置]，生成联动码。



步骤3.登陆AC管理端，在[终端行为安全/终端安全联动]页面，选择跟联动设备通信的IP地址后，点击生成联动授权码。

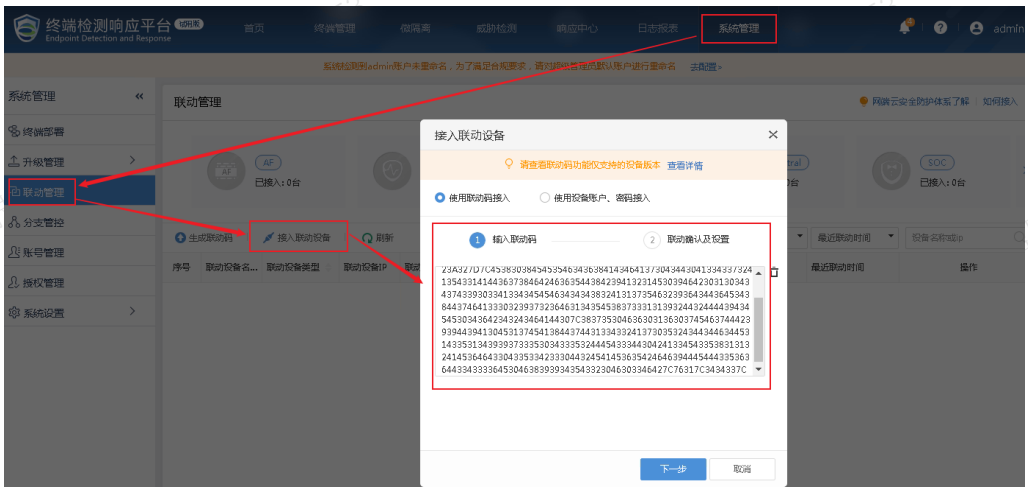
说明

：

每个联动码仅可使用一次，有多台联动设备接入时，需要为每一台联动设备重新生成一个联动码。

接入联动设备配置

步骤1.登录EDR管理平台，在[系统管理/联动管理]页面，点击接入联动设备，粘贴aTrust上生成的联动码，点击<下一步>后可以读取到aTrust的连接信息，选择与aTrust控制器通信的IP地址后点击确定即可。



步骤2.配置完成后，点击【连通性测试】测试联动配置是否成功。

步骤3.通过SDP也可以看到EDR联动状态已经成功。

说明：

EDR如需接入AC设备，联动接入过程与上述基本一致。

步骤4.登录AC管理页面，在[终端行为安全/终端安全联动]页面，点击接入联动设备，粘贴aTrust上生成的联动码，点击<下一步>后可以读取到aTrust的连接信息，选择与aTrust控制器通信的IP地址，配置联动设备名称后点击确定即可。

步骤5.配置完成后，点击【连通性测试】测试联动配置是否成功。

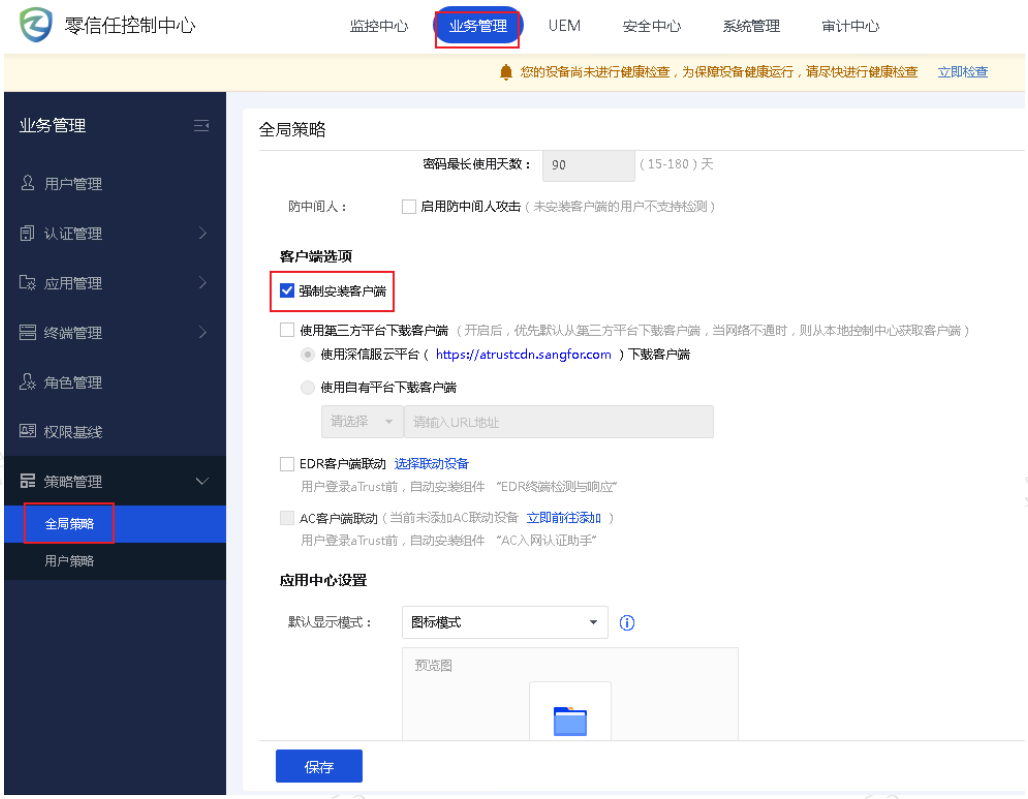
步骤6.通过SDP也可以看到AC联动状态已经成功。

说明：

联动对接任意一方作为主动连接设备都可以，例如也可以在EDR、AC生成联动码，在aTrust控制器识别联动码生成关联关系。

启用集成策略配置

步骤1.在aTrust管理端[业务管理/策略管理/全局策略]页面，勾选[强制安装客户端]开启终端强制安装。



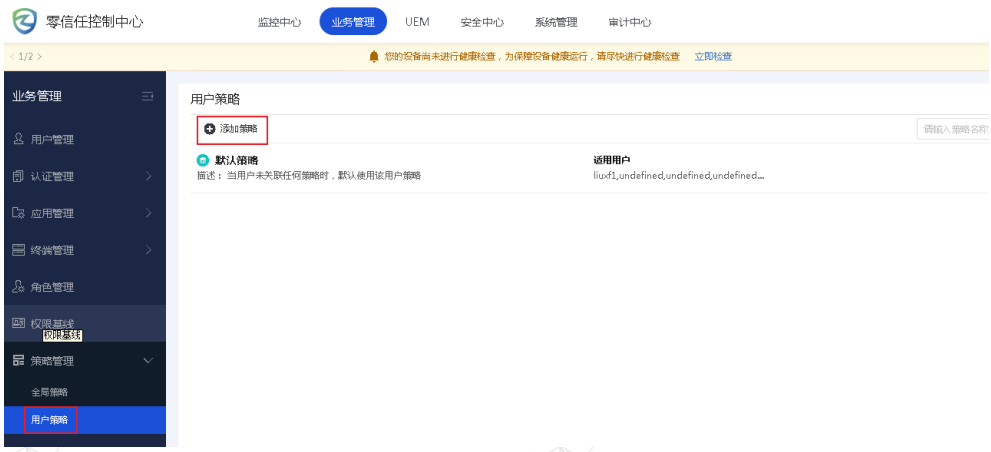
说明：

如果不开启强制安装客户端，纯WEB资源环境下不会主动推送aTrust客户端。

步骤2.aTrust可以设置全局推送或者针对指定用户定向推送集成安装策略。

• 如果针对全部用户推广，可在全局策略勾选[EDR客户端联动]和[AC客户端联动]选项，并选择联动的EDR和AC。

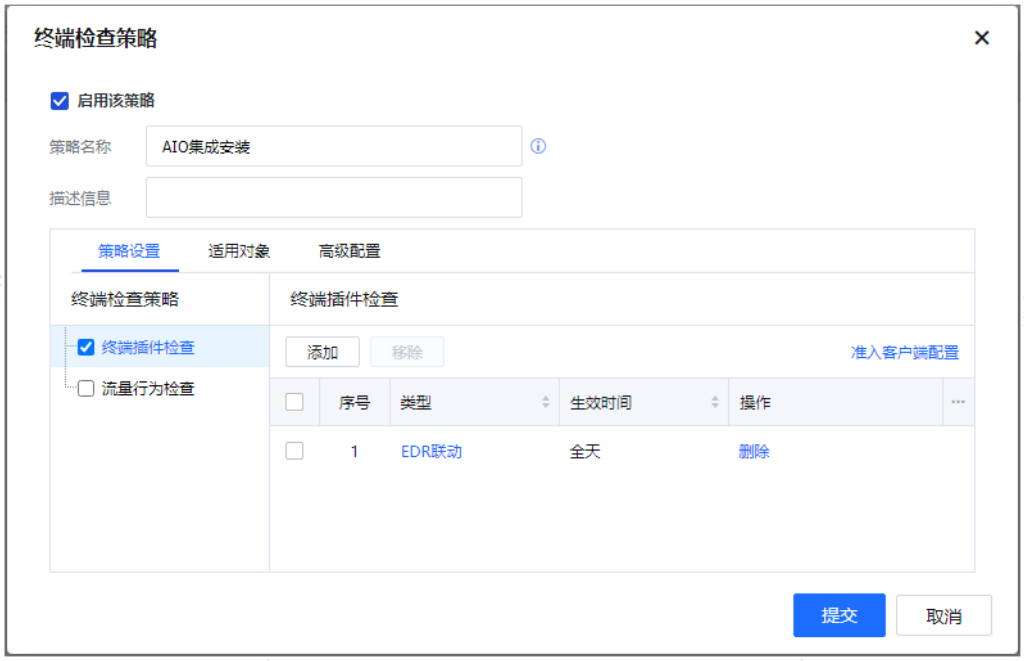
• 如果只针对部分用户推广，可以在aTrust管理端[业务管理/策略管理/用户策略]页面添加策略。



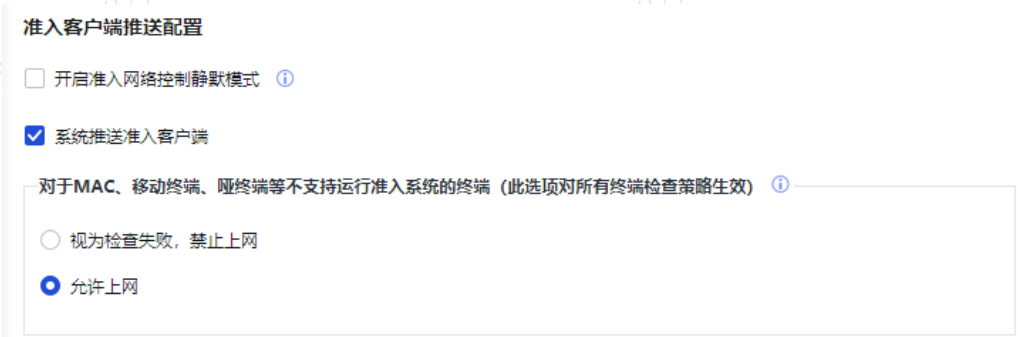
选择适用用户，[EDR客户端联动]和[AC客户端联动]选项，并选择联动的EDR和AC。

步骤3.在AC管理端[接入管理/终端管理/终端检查规则/插件检查规则]页面，新增[客户端集成规则]，输入规则名称、规则类型、规则描述，客户端需要集成的设备选择配置的联动的aTrust、EDR设备。

步骤4.在AC管理端[接入管理/终端管理/终端检查策略]页面，新增检查策略，将创建的EDR、aTrust集成规则关联给需要安装AIO客户端的用户。



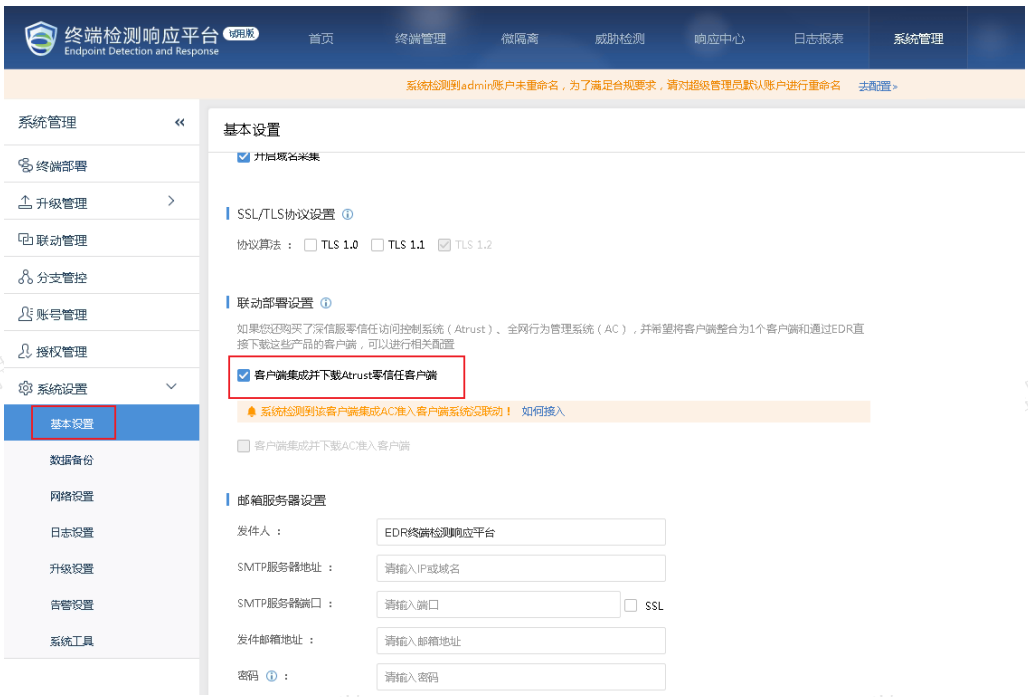
步骤5.在AC管理端[接入管理/终端管理/准入客户端配置]页面开启准入推送策略



说明：

如果以AC为起点安装客户端，当准入策略启用后，目标终端会显示准入安装页面，上网过程会中断直至准入安装完毕，建议开启策略前提前通知用户。

步骤6.用户如果需要通过先安装EDR再联动安装aTrust客户端，还需在[系统管理/系统设置/基本设置]页面勾选[客户端集成并下载aTrust零信任客户端]选项。



说明

：

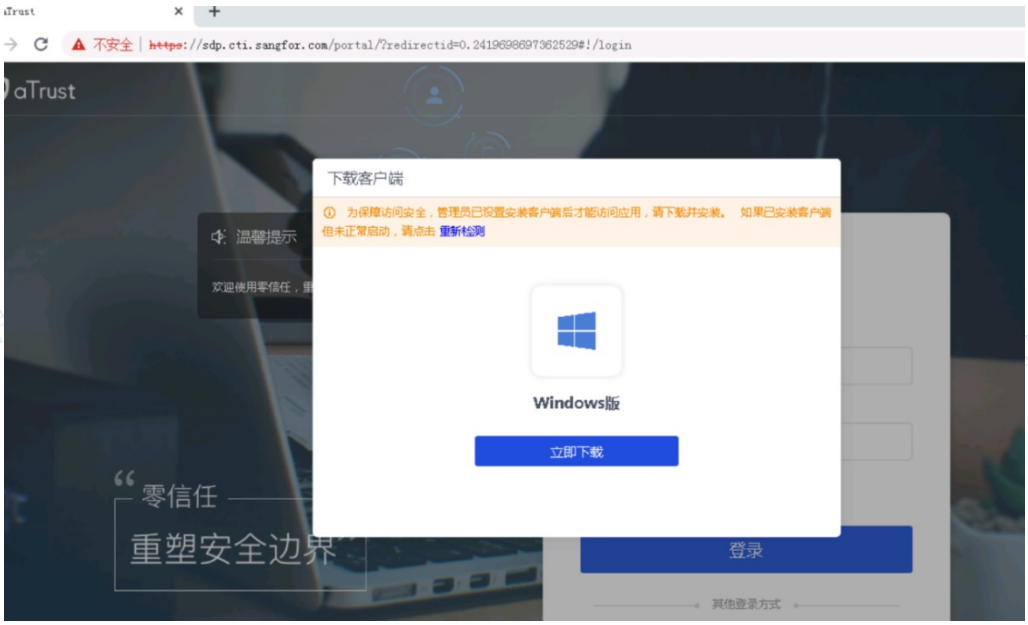
如果所有用户均通过aTrust登录客户端并联动下载EDR客户端，也可不开启该选项。

客户端使用

- 客户端安装

1. 全新安装场景(客户当前无aTrust、AC和EDR)，该场景面向用户新上aTrust、AC和EDR场景。

步骤7.当用户需要远程访问aturst代理的业务系统，提示用户需要安装aTrust客户端。



步骤1.下载安装完成后，可在客户端看到aTrust系统托盘。

步骤2.通过点击系统托盘图标或双击桌面快捷方式，可以打开客户端工作台，并在工作台上可以看到AC和EDR下载和安装进度。（由于EDR安装包比较大，内网环境需要等待5-10分钟，公网环境根据实际的带宽情况可能会比较久）。

说明：

如果没有开启全局策略，只开启了用户策略的话，需要对应用户认证登录成功以后才会联动下载AC和EDR。

步骤3.等待AC和EDR客户端安装完成后，在工作台可以看到AC[入网认证]选项，通过[安全]模块可以进行EDR客户端功能快捷操作和状态查看；系统aTrust托盘上会融合“终端检测响应”的图标。

2. 升级场景(客户当前有aTrust、AC和EDR客户端)，该场景面向已经部署过老版本aTrust、AC和EDR客户端的用户。

步骤1.首先需要升级aTrust控制器、代理网关和EDR至AIO版本，具体升级过程请参考各产品线升级操作指导。

步骤2.当用户接入aTrust发布的业务系统时，会提示客户端升级更新，点击立即更新。

步骤3.EDR默认开启终端自动更新，aTrust、AC和EDR均升级成功后，系统图标会融合成一个。

步骤4.aTrust升级为支持工作台的版本后，点击系统图标可以打开aTrust工作台。

说明：

由于EDR客户端升级包比较大，内网环境下升级预计5-10分钟，公网环境根据实际的带宽情况可能会比较久，升级过程需要耐心等待，可通过EDR管理平台查看终端升级状态。

---

3. 加装场景(客户当前有aTrust，但是没有EDR)，该场景面向已经部署aTrust客户端，新增部署EDR客户端的用户。

步骤1.用户如果部署的aTrust为非AIO版本，需要先完成aTrust设备升级，并完成EDR设备部署和联动配置，具体各项配置与前述基本一致。

步骤2.客户端登录aTrust后，aTrust会提示升级并在后台静默安装EDR客户端，EDR静默安装过程需要耐心等待。

步骤3.客户端升级安装全部完成后，客户端系统托盘会融合成一个，具体过程与新装和升级场景基本一致。

4. 加装场景(客户当前有EDR，但是没有aTrust)，该场景面向已经部署EDR客户端，新增部署aTrust客户端的用户。

步骤1.用户如果部署的EDR为非AIO本，需要先完成EDR管理平台升级，并完成aTrust设备部署和联动配置，各项配置与前述基本一致。

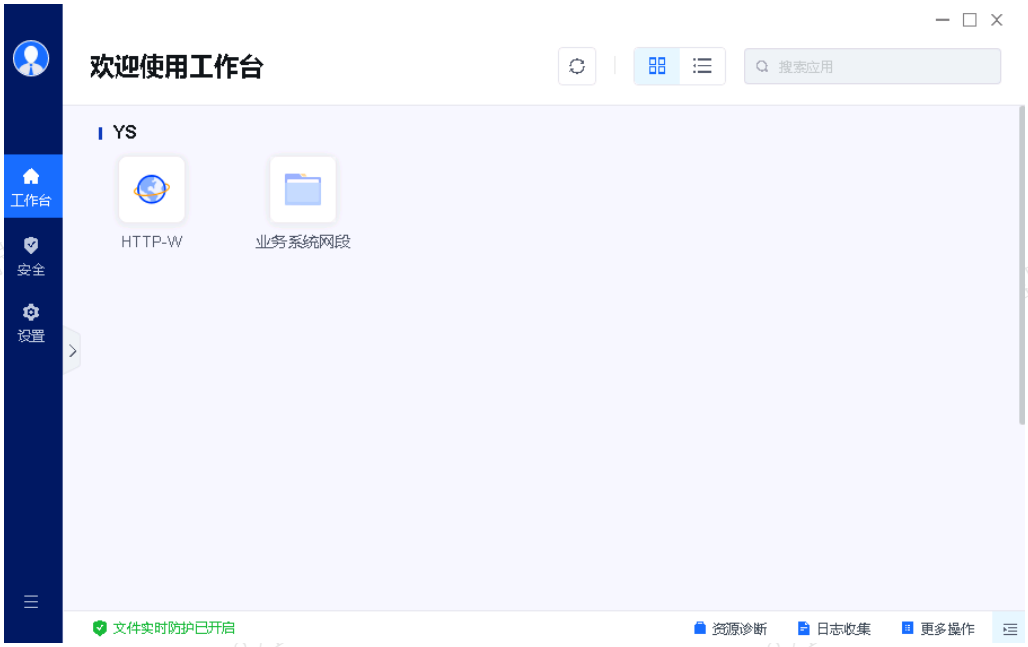
步骤2.EDR平台升级完成以后，客户端会自动静默升级，升级过程需要耐心等待。

步骤3.EDR管理平台如果同步开启了[客户端集成并下载aTrust零信任客户端]选项，客户端更新成功后会自动在后台静默安装aTrust客户端。

步骤4.客户端升级安装全部完成后，客户端系统托盘会融合成一个，具体过程与新装和升级场景基本一致。

• 客户端使用

1. 在atrust工作台点击【开始办公】即可接入atrust，认证后可访问业务系统。

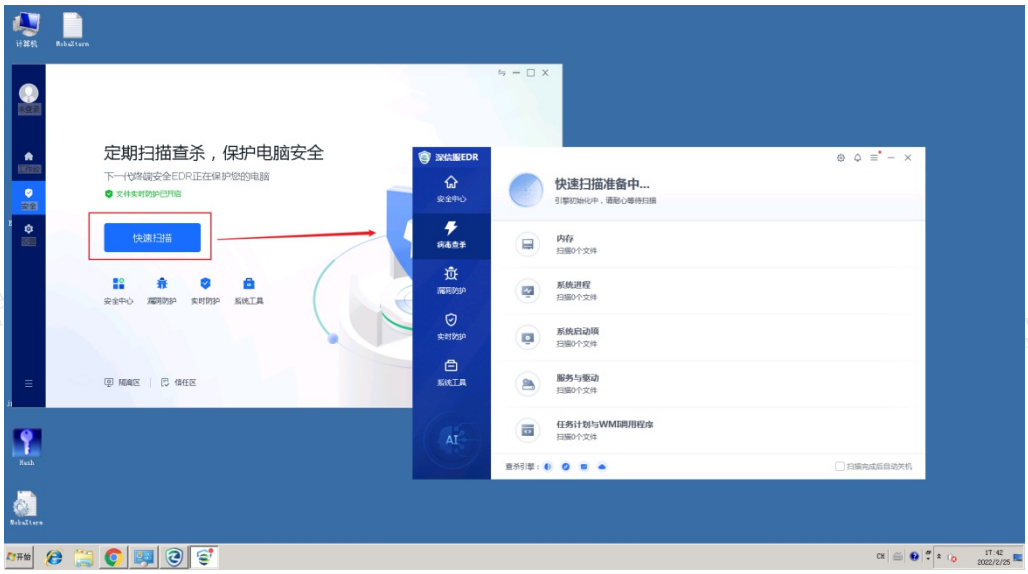


说明

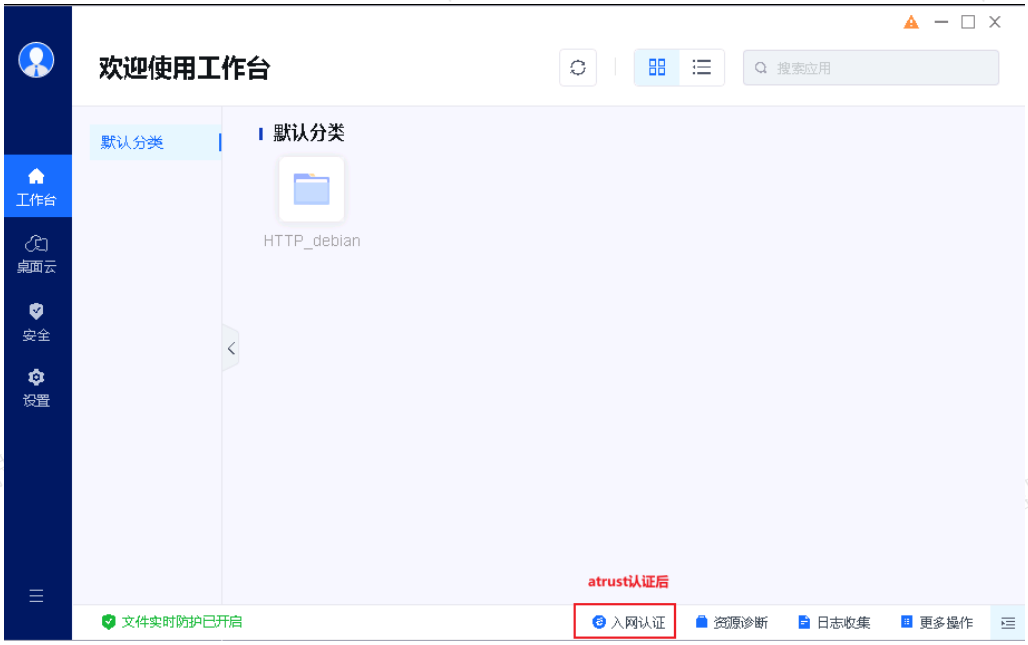
：

工作台不支持第三方认证和证书认证，包括：证书认证、LDAP认证、CAS、OAuth认证等。如需使用,在工作台选择对应认证时，会调出浏览器打开认证页面。

2. 在[安全]模块页面，点击对应的功能会直接调出EDR客户端页面执行相应的任务。



3. 点击【入网认证】选项，可以打开AC认证客户端界面。

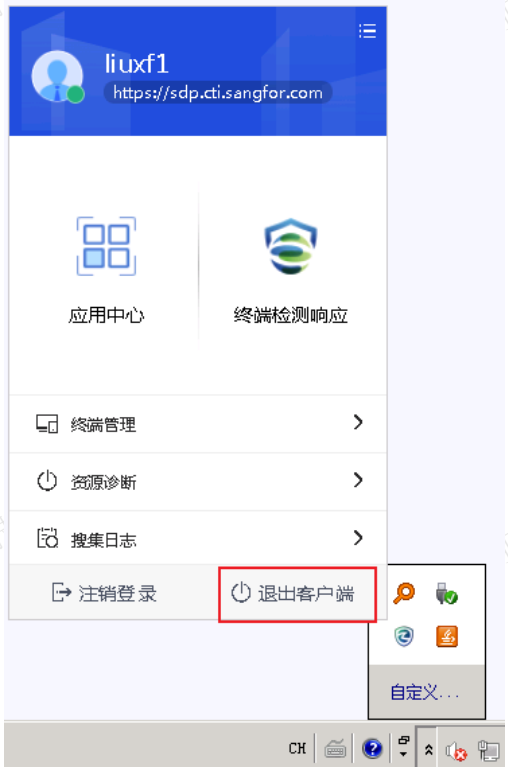


4. 通过系统托盘图标也可以调用对应的功能模块进行客户端操作。

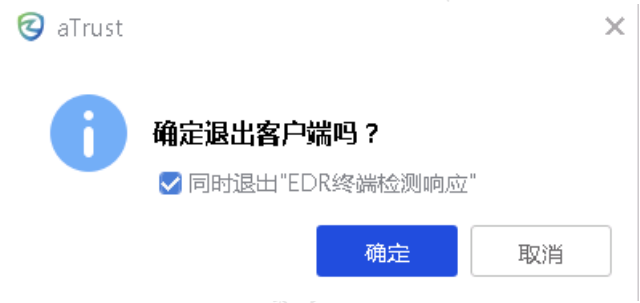
- 客户端退出

整体退出

1. 右键点击系统托盘，点击退出客户端选项。



2. 在对话中选择同时退出“EDR终端检测响应”，可以同时退出aTrust、AC和EDR客户端。



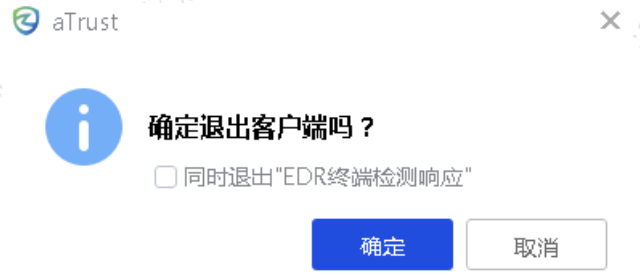
3. EDR客户端退出需要输入防护密码，需要由管理员提供，输入密码后即可整体退出客户端。

说明：

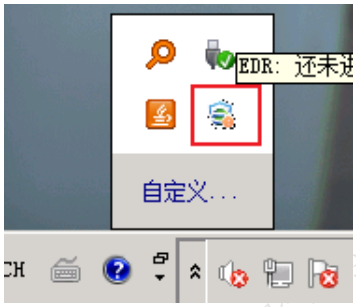
客户端完整退出后，重新打开aTrust工作台，此时只会拉起独立的aTrust客户端，需要手动拉起EDR客户端，工作台上才会融合EDR安全模块。同理，如果只单独打开EDR客户端，也只会开启EDR独立客户端。

分开退出

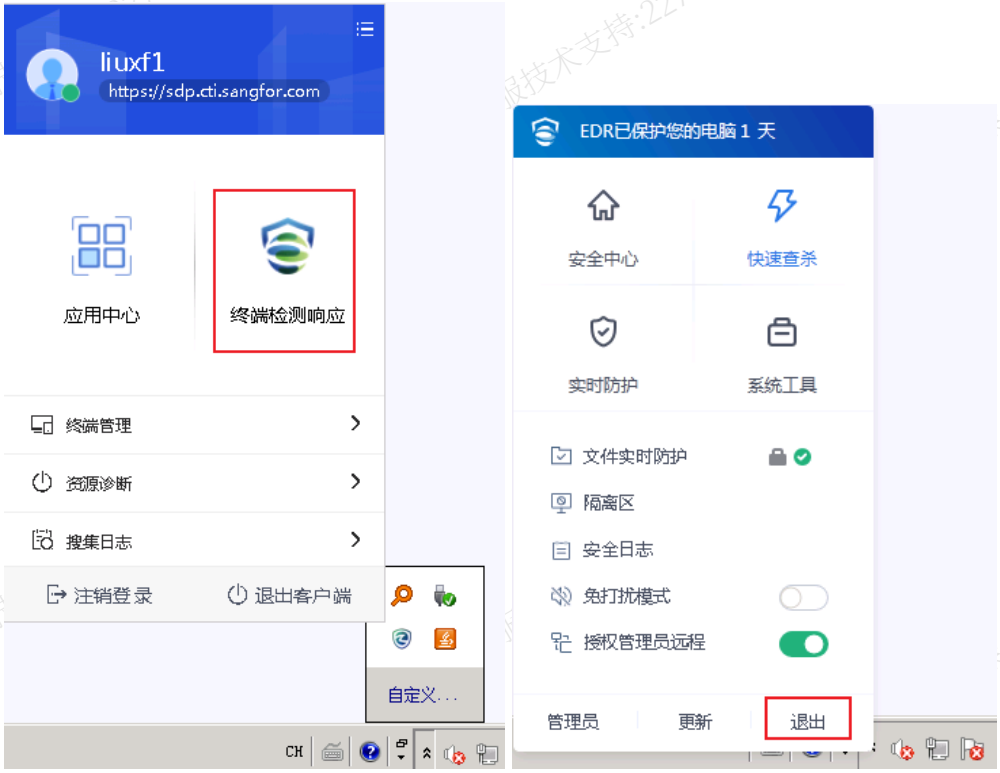
1. 右键点击系统托盘，点击退出客户端选项，在对话中缺省**不选择**同时退出“EDR终端检测响应”选项，可单独退出aTrust客户端。



2. 退出aTrust客户端后，系统托盘将变更为EDR独立客户端托盘。



3. 如需单独退出EDR，可点击进入EDR托盘图标以后，再点击退出选项，即可单独退出EDR客户端。



- 客户端卸载

当前版本各产品线卸载相互独立，互不干扰。

注意事项

1. AIOv3.0版本当前仅支持windows PC版本中文操作系统，暂不支持MAC、linux以及windows server版操作系统，各产品线兼容列表如下。

产品线	Win XP	Win 7	Win 8	Win 8.1	Win 10	Win 11
EDR	Y	Y	Y	Y	Y	Y
AC	N	Y	Y	Y	Y	Y
aTrust	N	Y	N	N	Y	Y

2. 用户如果手动卸载客户端以后，注册表会保留已安装过的标记，重新安装任意客户端AIO将不再联动下载安装其他客户端，避免用户手动卸载后重复推送，如果用户想重新安装其他客户端，也需要手动下载安装（如需恢复联动下载，可在注册表删除软件安装标识HKEY_LOCAL_MACHINE\SOFTWARE）。
3. AC主主、主备模式场景下，因为联动ID集群模式为一个，当主节点异常使得另一台节点工作并以新节点管理IP+联动ID与EDR或atrust建立互信时，因为管理IP变化会被拒绝，因此当前版本暂不建议在AC高可用环境下使用AIO集成安装策略。
4. aTrust、AC和EDR联动环境感知场景下，如果安全策略条件为运行指定杀毒软件为“Sangfor Defender 防病毒程序”，客户端手动卸载EDR后，仍能命中安全策略，原因是EDR卸载没有清理Windows安全中心标记，SDP会认为还是安装了EDR，客户端手动重启系统后，会自动清理该标记。
5. aTrust、AC和EDR联动环境感知场景下，aTrust只开启了环境感知评分，未开启用户必须安装EDR的准入策略，如果用户是首次安装aTrust、AC和EDR客户端，用户登录aTrust完成客户端安装后，由于EDR安装尚未完成，aTrust暂时无法获取终端评分，缺省用户评分为100分。
6. aTrust、AC和EDR联动环境感知场景下，aTrust只开启了环境感知评分，未开启用户必须安装EDR的准入策略，如果aTrust控制器与EDR管理平台不通，aTrust也无法获取终端评分，缺省用户评分为100分。
7. 用户环境如果部署了多台EDR管理平台并接入到SDP，如果客户端登录时全局策略联动的EDR设备为A，客户端登录以后，管理员修改全局策略联动的EDR设备为B，SDPC会从EDR-B设备获取评分，导致客户端真实评分失真。
8. 当前AIO1.0与AIO2.0不兼容，不可以使用不同迭代版本的产品线开启联动，例如atrust2.1.17版本目前仅合入AIO1.0，所以不支持与EDR3.5.18开启联动。
9. AIO3.0向下兼容2.0，可与2.0版本联动，例如atrust2.2.6版本支持和edr3.5.18-24配置aio联动。
10. EDR PC基础版的授权不支持AIO联动，其他PC高级版、全量版、服务器旗舰版、全量版均支持AIO，探针版也支持AIO，不过探针版没有托盘统一。

XDR平台对接

安全管理员需要一种方法能够在分析安全事件时快速定位到资产责任人，这样在进行事件深入调研和处置时，可以快速与资产责任人取得联系和授权，提高处置效率，减少时间损耗。AC可与SaaS-XDR和分布式XDR进行联动对接，同步在线用户，实现资产人机对应。

SaaS-XDR联动对接

实现效果

通过建立SaaS-XDR和AC联动对接，SaaS-XDR主动向AC发起获取在线用户信息请求（默认5分钟），实现资产人机对应。

前置条件

1. 客户已有云图账号并购买SaaS-XDR（可扩展检测响应平台XDR）。

2. AC已完成基础网络部署，并完成认证策略配置，在线用户管理可查看上线用户信息。

端口矩阵

方向	需要放通IP/域名	需要放通端口	用途
AC->SaaS-XDR	device.scloud.sangfor.com.cn device.sangfor.com.cn	TCP443 TCP5000	
AC->SaaS-XDR	dlauth.sangfor.com.cn	TCP443	
AC->SaaS-XDR	datalake.sangfor.com.cn	TCP443	
AC->SaaS-XDR	xlink.sangfor.com.cn	TCP443	

功能配置

步骤1.登录深信服云图https://x.sangfor.com.cn，在首页[安全产品/可扩展检测响应平台XDR]进入SaaS-XDR平台，在导航栏[配置管理/产品接入]中新增设备，“设备类型”选择AC后会自动生成配置（也可以自行修改），点击<复制认证信息并确定>。

步骤2.登录AC设备，在导航栏[安全管理/终端安全联动]点击“接入联动设备”,在接入联动设备中选择“设备账号、密码接入”，点击<粘贴认证信息>，将在SaaS-XDR复制的认证信息粘贴到此处，点击提交。

步骤3.在AC设备[安全管理/终端安全联动]中可查看AC和SaaS-XDR联动状态。

步骤4.在AC设备[系统管理/系统配置/高级配置/加入集中管理设置]中可查看AC加入云图状态。

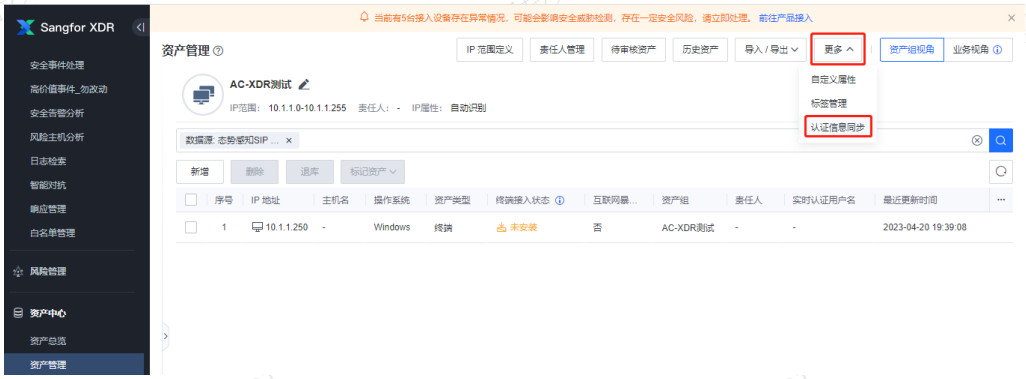
步骤5.在SaaS-XDR平台[配置管理/产品接入]中可查看接入AC状态。

效果展示

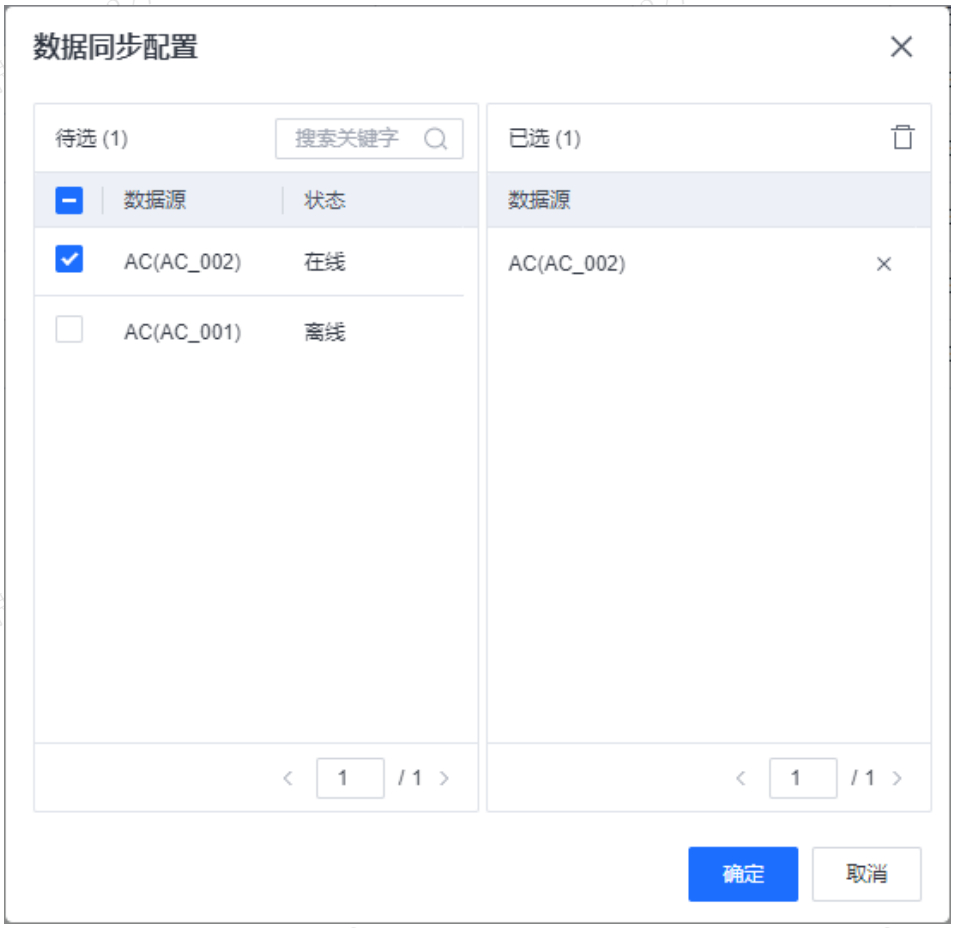
步骤1.在AC设备[全网监控/入网用户管理]可查看已上线用户信息。

步骤2.未进行认证信息同步前，在SaaS-XDR导航栏[资产中心/资产管理]可查看资产“实时认证用户名”为空。

步骤3.在SaaS-XDR资产管理页面选择“认证信息同步”。

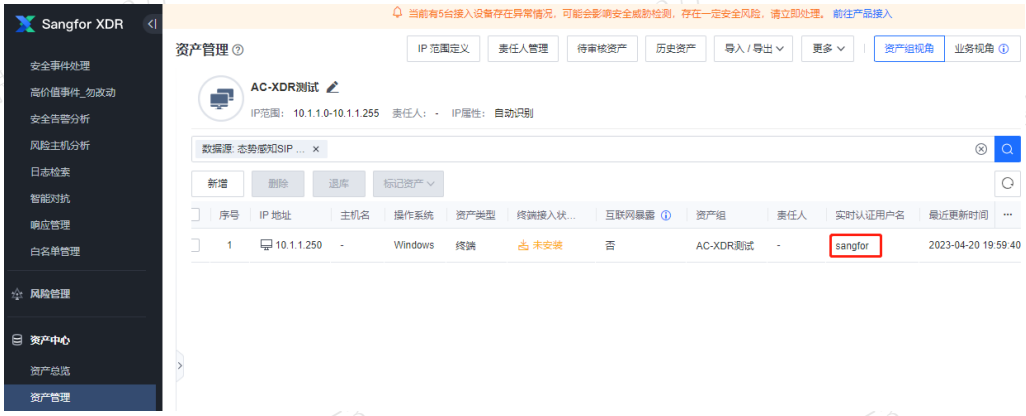


步骤4.点击“数据同步配置”，选择需要同步的AC设备，点击<确定>。



步骤5.点击“立即同步”后，SaaS-XDR向AC主动请求在线用户信息。

步骤6.在SaaS-XDR导航栏[资产中心/资产管理]可查看资产“实时认证用户名”为sangfor。



分布式XDR联动对接

实现效果

通过建立分布式XDR和AC联动对接，分布式XDR主动向AC发起获取在线用户信息请求（默认5分钟），实现资产人机对应。

前置条件

1. 客户已部署分布式XDR。
2. AC已完成基础网络部署，并完成认证策略配置，在线用户管理可查看上线用户信息。

端口矩阵

方向	需要放通IP/域名	需要放通端口	用途
AC->分布式XDR	分布式XDR集群业务口	TCP443	数据上报端口
AC->分布式XDR	分布式XDR集群业务口	TCP19666	长连接端口

功能配置

步骤1.登录深信服分布式XDR，在导航栏[配置管理/产品接入]中新增设备，“设备类型”选择AC后会自动生成配置（也可以自行修改），点击<复制认证信息并确定>。

步骤2.登录AC设备，在导航栏[安全管理/终端安全联动]点击“接入联动设备”,在接入联动设备中选择“设备账号、密码接入”，点击<粘贴认证信息>，将在分布式XDR复制的认证信息粘贴到此处，再填入分布式XDR的IP地址，点击提交。

步骤3.在AC设备[终端行为安全/终端安全联动]中可查看AC和分布式XDR联动状态。

步骤4.在AC设备[系统管理/系统配置/高级配置/加入集中管理设置]中可查看AC加入云图状态。

步骤5.在分布式XDR平台[配置管理/产品接入]中可查看接入AC状态。

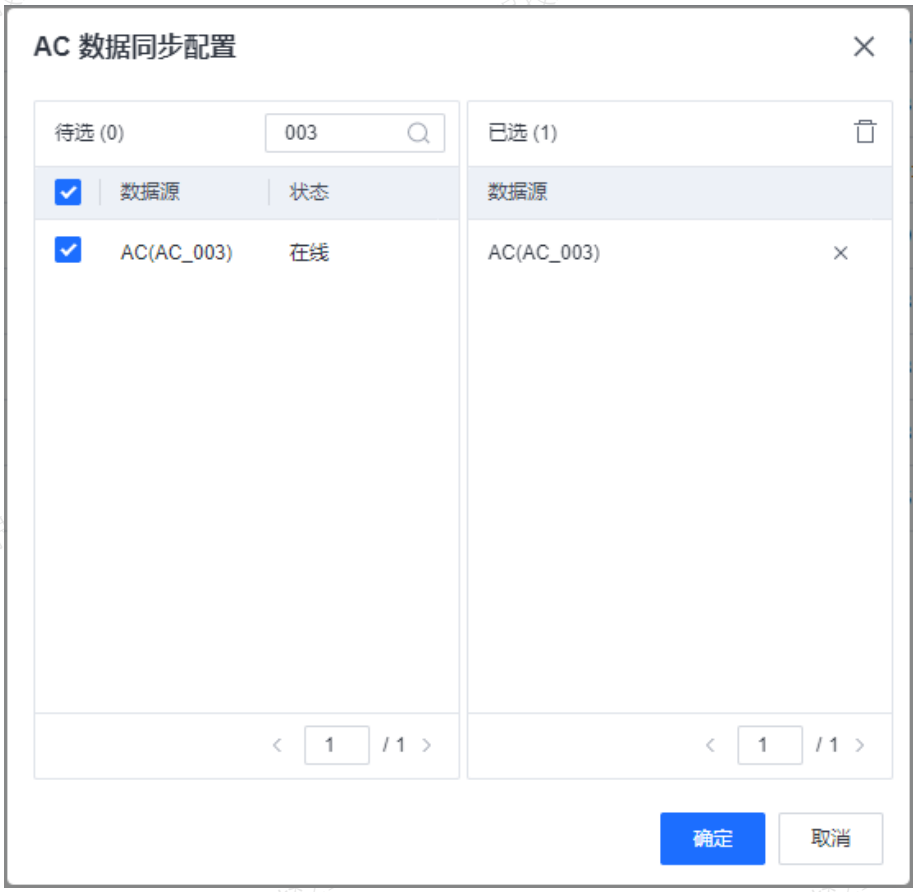
效果展示

步骤1.在AC设备[全网监控/入网用户管理]可查看已上线用户信息。

步骤2.未进行认证信息同步前，在分布式XDR导航栏[资产中心/资产管理]可查看资产“实时认证用户名”为空。

步骤3.在分布式XDR资产管理页面选择“认证信息同步”。

步骤4.点击“数据同步配置”，选择需要同步的AC设备，点击<确定>。



步骤5.点击“立即同步”后，分布式XDR向AC主动请求在线用户信息。

步骤6.在分布式XDR导航栏[资产中心/资产管理]可查看资产“实时认证用户名”为sangfor。

注意事项

1. 由于AC集中管理只能加入BBC或云图，当AC和SaaS-XDR/分布式XDR联动对接时需要使用云图接口，所以已经加入BBC的AC需要解除BBC集中管理后才能完成对接。
2. 一台AC设备只可对接一台XDR（一台SaaS XDR或者一台分布式XDR）。
3. AC设备的系统时间需要和XDR的系统时间保持一致，误差在5分钟内。

系统管理

对象定义

对象是具备某些公共特性的元素集合，将对象在行为审计、流量管理的配置项中引用对象。包括：应用特征识别库、应用智能识别库、自定义应用、URL分类库、网络服务、IP地址库、时间计划组、关键字组、文件类型组、位置对象组、业务定义等。

表23对象定义功能说明

操作	功能说明
应用特征识别库	应用特征识别库定义了网络中大部分的应用协议，用来检测和识别上网数据的应用协议，根据数据包的特征字或者协议、端口等匹配条件来检测应用协议，能够很好的检测出通过端口或协议无法区分的应用协议。
应用智能识别库	用于识别各种网络中数据的应用类型，它和应用特征识别库的判断方式有所不同，可以识别一些加密的数据。如明文或密文等形式P2P应用、skype、SSL、SANGFOR VPN数据的识别、Web在线代理、皮皮影视等。
自定义应	当特征识别库无法满足对流量的应用控制需求，或者需要对流量进行更精准的控制时，可以通过指定协议类型、源端口、目的端口、特征字来配置自定义应用协议实现流量控制。

用	
URL分类库	URL分类是具有相同特征的URL集合。URL分类包括两种：预定义分类和自定义分类，预定义分类由深信服安全中心提供并维护，自定义分类由用户自行配置和维护。
网络服务	用户可通过端口号和协议等条件设置网络服务，并且通过数据包的端口和协议来对上网数据进行控制。
IP地址库	IP组是IP地址的集合，包括ISP地址库、国家地区设置，将IP地址加入IP组可以方便维护和被其他配置项中引用。
时间计划组	时间段包括“时间段有效期”和“周期时间段”，配置时间段可方便其他配置项指定生效时间。
关键字组	通过关键字组，将关键字分组集中管理，方便在[行为管理/访问权限策略/web关键字过滤]中引用。
文件类型组	文件类型组将用户使用到的文件类型统一管理和维护，方便在[行为管理/访问权限策略/WEB过滤/文件类型过滤]中限制HTTP和FTP的文件上传和下载，也可用于[流量管理/流控策略/带宽分配]的规则中设置文件类型上传下载的流量控制，行为审计的互联网审计策也能进行引用。
位置对象组	用于设置位置对象组关联的适用对象组，位置对象组是用于通过IP段或VLAN类型划分不同位置。可以被权限管理、流控策略的章节引用。。
业务定义	业务定义用于设置业务组关联的业务对象，方便在在[行为审计/业务审计策略]中被引用。

应用特征识别库

在[系统管理/对象定义/应用特征识别库]，可以查看所有的特征识别库，启用和禁用特征识别库，当前设备可识别的应用总数和规则总数。应用识别库是根据数据包的特征值、协议、端口、方向、长度、内容等多个条件来检测数据包的应用类型，能够很好的检测通过端口和协议，无法区分的应用类型，如QQ、P2P等。

应用特征识别库有内置和自定义两种。内置的识别规则无法进行编辑和删除，部分应用可以禁用，涉及到基础协议判断的应用不能被禁用。自定义规则库可以进行增加、删除、修改等操作。

如需更新内置规则库需要序列号授权，请到[系统管理/系统配置/授权管理]页面查看

应用识别&URL库升级授权的序列号状态是否有效，在有效期内且设备正常联网的情况下，设备可定时更新最新的规则库。

自定义标签管理：对设备默认的应用标签进行导入和导出操作，不能删除和编辑。

也可添加自定义的应用标签。并且对自定添加的标签进行删除和编辑。

新增一个应用标签，点击<添加>打开新增标签，填写自定义名称和描述，选择关联应用，选择需要限制的应用，点击<提交>即可。

应用智能识别库

应用智能识别库是用于识别各种上网数据的应用类型，它和应用特征识别库的判断方式有所不同，可以识别

一些加密的数据。如明文或密文等形式P2P应用、skype、SSL、SANGFOR VPN数据的识别、Web在线代理、皮皮影视等。

应用智能识别能显示应用名称、应用类型、标签和应用规则状态。管理员可勾选应用名称对应的复选框进行启用和禁用该类型的规则。

应用智能识别库还能对应用名称为蓝色的标题的应用编辑操作，例如编辑“P2P行为”这个应用规则的内容。点击<P2P行为>弹出编辑框。

勾选<是否启用该规则>，其中内容框为置灰的选项是不能编辑，规则配置选项中的检查灵敏度和排除扫描端口可进行编辑。

[检测灵敏度]：对规则的灵敏度设置，可设置为高、中、低、极低四项。智能识别P2P可能存在误判，所以通过灵敏度来设置判断的标准，从“高”级别到“极低”级别灵敏度依次降低。用户可以根据具体数据的识别情况来调整灵敏度级别。

• 如果有大量未识别的数据，且数据连接的端口都是随机的端口和目标地址不确定的情况，这些数据可能是未识别的P2P数据，可将灵敏度设置高一些。

• 如果一些应用本不是P2P的数据，却被识别成P2P，可能是灵敏度级别设置高了，可以将灵敏度设置低一些

。

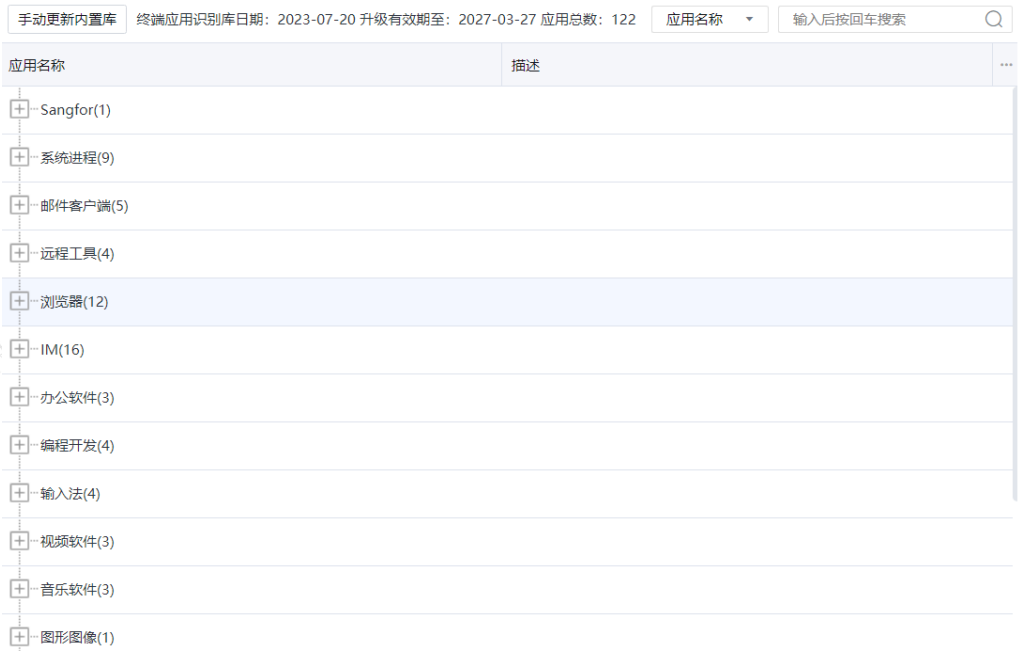
[排除扫描端口]：设置排除端口项，数据的目标端口是排除端口的话，设备将不会对此类数据进行P2P智能识别，能避免误判的情况。

终端应用库

终端应用库适用于[终端检查策略]中的[应用联网管控规则]、[终端防泄密]的[文件外发管控]、以及[客户端审计策略]的[客户端应用审计]，终端应用库有内置和自定义两种。内置的识别规则无法进行编辑和删除，自定义规则库可以进行增加、删除、修改等操作。

内置终端应用库

内置终端应用库可查看当前设备可识别的应用总数和规则总数。如需更新内置规则库需要序列号授权，请到[系统管理/系统配置/授权管理]页面查看应用识别&URL库升级授权的序列号状态是否有效，在有效期内且设备正常联网的情况下，设备可定时更新最新的规则库。



自定义终端应用库

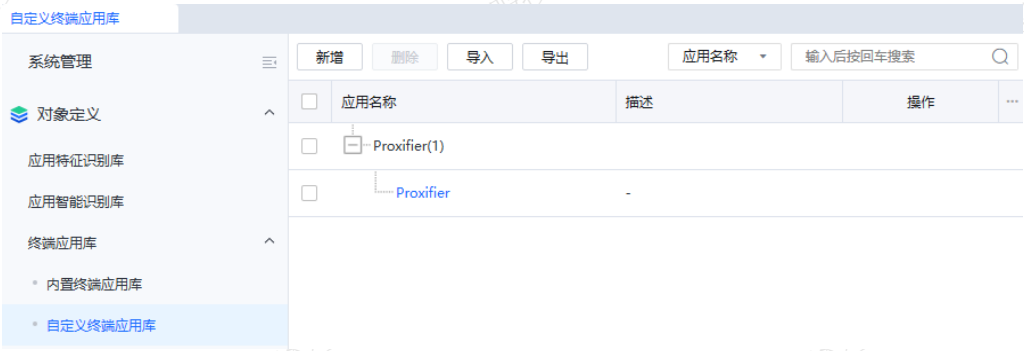
自定义终端应用是用于自定义终端应用特征识别规则，可以定制设备内置终端应用库中未包含的应用。

自定义终端应用库

1. 在[系统管理/对象定义/终端应用库/自定义终端应用库]新增自定义应用，点击“应用特征获取指南”可下载应用特征识别工具和应用特征获取指南文档。

2. 双击打开app_tool，将应用桌面快捷图标（或 exe） 拖拽到“蓝色方框区域”，复制识别到的应用特征信息（点击“复制”按钮进行复制操作）

3. 重新回到【系统管理/对象定义/终端应用库/自定义终端应用库】页面，新增自定义应用，将在app_tool识别到的应用特征信息粘贴到应用特征框，然后点击“一键添加”，应用特征参数栏则显示添加成功应用，点击“提交”完成自定义应用添加。



自定义应用

自定义应用是用于自定义应用特征识别规则，可以定制设备内置的应用特征识别库中没有的应用，自定义的应用可以通过数据包方向、协议号、目的端口、IP地址、目标域名。在导航菜单页面中的[系统管理/对象定义/自定义应用]页面，可对自定义应用进行新增、删除、启用和禁止、导入和导出自定义应用等操作。

操作场景

需要对公司的邮件做流量保证，但是选择应用类型的时候无法单独选择公司邮件，这时候可以自定义一个公司邮件的应用。

操作步骤

步骤1.勾选<用户自定义类别优先>，启用该功能后设备会优先走自定义类型的应用。

步骤2.并设置应用基本信息，设置规则名称，描述信息，以及应用类型和应用名称（直接在输入框输入自定义类型和名称或者选择之前定义的类型和名称）。

步骤3.设置匹配数据包特征类型。

- 数据包方向：设置数据通过设备的方向，匹配到此方向的才会继续往下识别。
- 三层协议：设置数据所采用的协议类型，此例中邮件发送是TCP协议。
- 目标端口：设置数据所访问的目标端口，此例中邮件发送是TCP 25端口。
- IP地址：设置源IP、目标IP或者是代理识别后的目标IP。

• 匹配目标域名：设置数据包访问的目标域名地址，此例中设置公司的域名邮箱地址，比如“mail.sangfor.com.cn”。

步骤4.设置完成后点击<提交>，完成此条规则的设置。

步骤5.设置用户自定义的规则优先级：因为内置应用特征识别库中也有邮件的识别规则，如果内置的规则优先的话，数据可能会优先匹配到内置的邮件规则，而不会匹配到“公司邮件”这条自定义的规则了，所以此处要设置自定义的规则优先匹配。在自定义应用页面勾选[用户自定义规则优先]即可。

说明

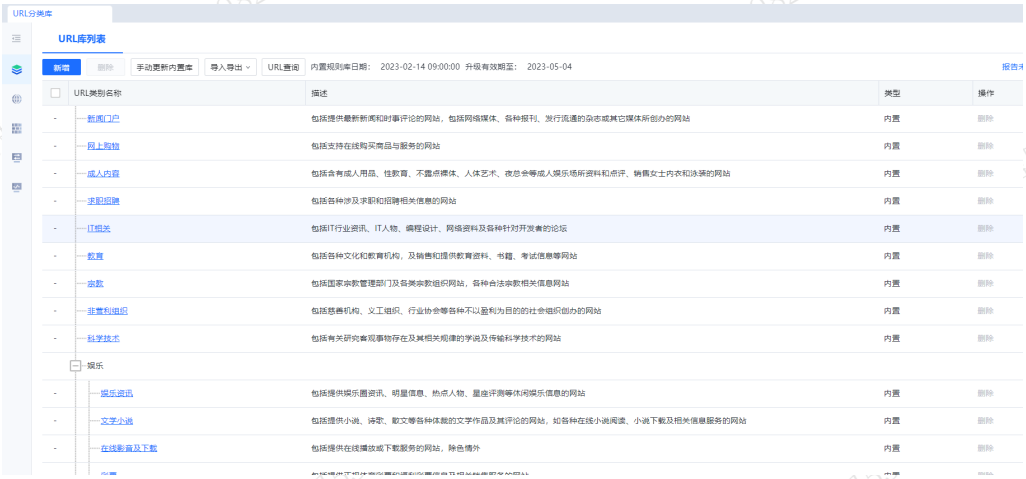
：

建议设置自定义规则时要加上目标端口、IP和域名等识别信息，如果识别的条件过于宽泛，可能会和内置的应用识别规则有冲突导致应用识别混乱，而导致部分控制和审计失效。

URL分类库

URL分类库是根据网页的内容定义出不同的URL类型，帮助设备识别各类网站，来实现对各种类型的网站的访问权限控制和流量控制。URL分类库也被复用到应用特征识别库中，当需要对内网用户访问网站的类别进行过滤，可在[行为管理/访问权限策略/应用控制]中进行设置。

在[系统管理/对象定义/URL分类库]，可显示URL库列表信息，包括内置的URL库和用户自定义的URL库。如需更新内置规则库需要序列号授权，请到[系统管理/系统配置/授权管理]页面查看应用识别&URL库升级授权的序列号状态，在有效期内，且设备正常联网的情况下，设备可定时更新最新的规则库。



说明

：

1．URL查询不支持模糊查询。

2．自定义URL组导入是同名覆盖，不是新增的方式，新导入的URL组与已有的URL组同名情况下会被覆盖；如果新导入的URL组与已有的URL组不同名，则作为新增URL组处理。

自定义URL组是在内置URL组不满足需求时，管理员可以新增自定义URL组。管理员可对自定义URL分类库如下操作。

表24URL分类库功能说明

操作	功能说明
新	点击<新增>会弹出新增URL类型框，输入URL组名称、描述，URL：添加需要设置的URL，可同时包含多个，可支持通配符。域名关键字：根据URL中的关键字自动匹配URL组，访问

增	域名中包含所设置的关键字则被识别成该URL组，域名关键字匹配优先级低于内置URL库和自定义URL库。
删除	用户可以删除自定义的URL组，设备内置的URL组不能删除。
修改	对用户自定义的URL组和设备内置的URL组的权限不一致。 对用户自定义的URL组可修改组域名、URL、关键字、描述等。 对设备内置的URL组只能编辑编辑URL和关键字作为补充。
URL查询	点击URL查看，填写需要查询的域名，点击<查询>会显示URL对象的类别。
手动更新规则库	点击手动更新内置库，选中内置文件库打开即可。
导入/导出	点击导入导出，选中<导出自定义的URL组>选中保存路径和文件名，则导出所有自定义URL组内容。选中<导入自定义的URL组>，上传CSV格式的文件。 **注意：**当导入的文件组与已有的同名则会被覆盖，不同名作为新的URL组处理。

网络服务

网络服务用于定义各种服务，包括端口和协议，用于确定防火墙的过滤规则和根据已定义的服务来确定上网的权限。

防火墙的过滤规则可在[防火墙/过滤规则]中设置，确定上网权限是在[行为管理/访问权限策略/应用控制/端口控制]中设置。

在[系统管理/对象定义/网络服务]可对网络服务进行新增、编辑、删除等操作。

管理员可点击<新增>，会弹出[新增网络服务]窗口，输入服务名称，服务配置包括TCP、UDP、ICMP、其他，并选择对应的协议则在窗口中添加对应的端口。其他可写协议号，协议号0表示所有的协议。点击<提交>可完成网络服务的配置。

IP地址库

IP地址库包括IP组、ISP地址库、国家/地区。

IP组

IP组用于定义一个包含某些IP地址的IP组，IP组可以是内网的IP段，公网的IP段、和全部IP段。IP组可以被以下模块引用：

- 在[系统管理/防火墙/过滤规则]，用于设定防火墙规则中的源IP、目的IP等。
- 在[接入管理/用户管理/组和用户/用户属性/基于IP或MAC识别]来定义内网用户。
- 在[行为管理/访问权限策略/应用控制/端口控制]中适应对像也能引用。
- 在[流量管理/流控策略]用于设置通道使用范围，设置目标IP组时可以引用。

在[系统管理/对象定义/IP地址库]，点击<新增>会弹出IP组设置窗口，需要填写IP 组名称、IP组描述，IP地址。

• **IP地址**：一行一个单个IP（IPV6）地址或IP（IPV6）地址范围，地址范围的格式为“起始地址-结束地址”，以IPv4为例：如“192.168.0.1-192.168.0.100”。

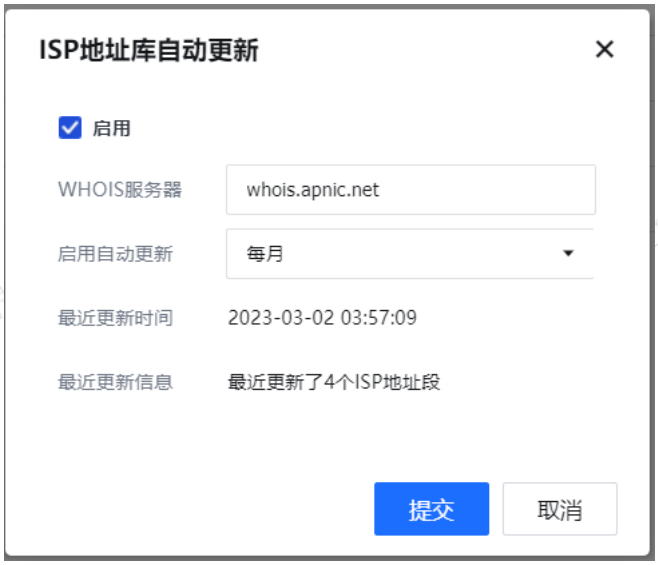
• **解析域名**：是通过联网进行解析，要求电脑能正常上网，将某些域名对应的IP地址，通过该功能可以自动将解析出来的IP地址追加到IP地址列表。该解析一次性的，在定义时进行解析，后续以解析出的IP地址匹配，而非时时解析。

ISP地址库

ISP地址库用于设置网络运营商的IP地址段，默认联通、电信、移动、教育网等，可应用在[系统管理/网络配置/链路负载]。

在[系统管理/对象定义/IP地址库]，点击<新增>会弹出ISP地址库设置窗口，需要填写名称、描述，IP地址和WHOIS标志。

- 名称：用于设置ISP名称。
- 描述：用于设置ISP地址库的描述信息。
- 地址范围：用于手动设置该运营商的网络IP段。
- WHOIS标志：用于设置相应的ISP地址段对应的WHOIS标志，便于根据标志识别不同运营商的地址。
- ISP地址库自动更新：可设置自动更新ISP地址库，默认启用。



- **WHOIS服务器**：可设置更新ISP地址库服务器。
- **启用自动更新**：可选择每天、每周、每月。
- **最新更新时间**：显示最近一次更新时间。

• **最新更新信息：**显示最近一次更新ISP地址段数量。

• 设备出厂默认有联通、电信、中国移动、教育网四个ISP地址库。

国家/地区

国家/地区内置了本地和国际的一些地址库，主要用于[流量管理/虚拟线路配置]虚拟网线模式中虚拟线路规则中选择外网IP时调用该地址库。

在对象定义里面选择[IP地址库/国家/地区]，点击<新增>一个国家地区的属性，填写名称，国家和地区根据需求选择即可。

点击<提交>添加成功在列表显示。

归属地查询

当内网检测到有异常流量，管理员可以通过[归属地查询]去定位IP的位置然后做相应的策略。点击<归属地查询>弹出IP归属地查询，输入IP地址，点击<查询>后会出现查询到的归属地结果，如“192.200.244.15”查询结果：美国。

归属纠正

当管理员检测内网的某个IP地址属于非所属区域时，可以通过[归属纠正]来修改IP的正确区域，点击<新增>IP的归属地纠正，输入IP地址/范围选择正确的归属地。

新增归属地添加如下图所示。

更新地址库

在设备联网的情况下，IP地址库能实时更新，也可以手动更新以获取最新的地址库，如果是已经最新，手动更新的时候会提示无需更新。

时间计划组

时间计划组是用于定义常用的时间组合，可应用在[系统管理/防火墙/过滤规则]、[行为管理/访问权限策略]、[行为管理/流量管理/流控策略]中能设置自定义时间段和规则的生效和失效的时间。

在[系统管理/对象定义/时间计划组]，显示当前设置的时间段，设备默认的时间段是周一至周日全天24小时，这条规则不能删除。管理员也能查看时间分布预览的情况，横轴为时间点，纵轴为日期范围。

点击<新增>，弹出时间计划组页面，填写名称和描述。

点击<配置>会跳转到日程配置页面，启用日程，有两种选择：生效日期和排除日期，可根据需求进行设置生效日期的时间段和排除日期的时间段，最多可设置十个。

说明：

生效日期是满足此日期才能匹配该时间计划组，排除日期是非此日期内的才满足该时间计划组，一般用于节假日。

关键字组

关键字组用于Web关键字过滤功能用于限制用户对某些关键字进行搜索和下载的操作，管理员可进行新增、删除操作。

关键字组主要是在[行为管理/访问权限策略/web关键字过滤]中调用。

点击<新增>弹出关键字编辑页面，填写名称和描述信息，在关键字输入框输入需要过滤的关键字字段信息，点击<提交>配置完成。

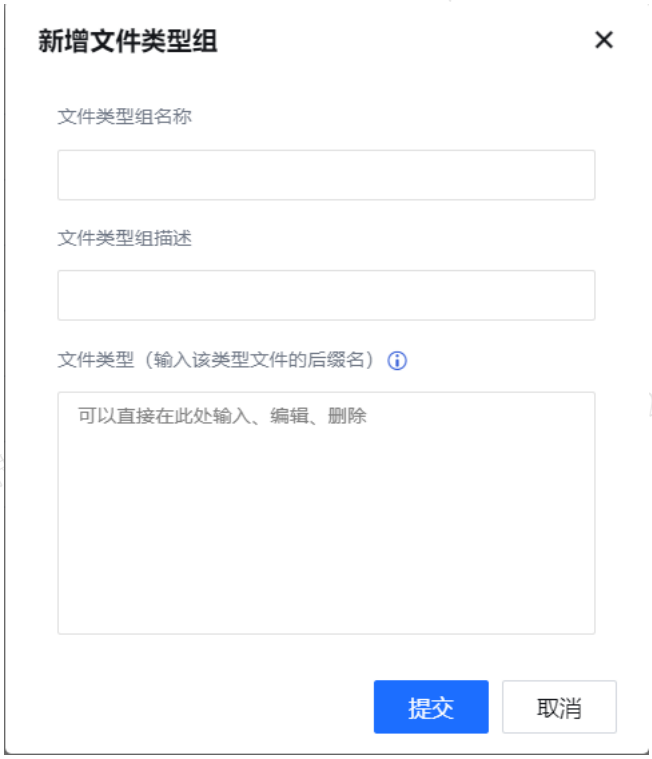
文件类型组

文件类型组用于定义需要的文件类型。

- [行为管理/访问权限策略/WEB过滤/文件类型过滤]中限制HTTP和FTP的文件上传和下载。
- [行为管理/流量管理/流控策略/带宽分配]的规则中设置文件类型上传下载的流量控制。
- [行为审计/上网审计策略]中的文件类型也能引用。

管理员可新增其他文件类型组合删除不需要的文件类型组。

点击<新增>弹出文件类型组页面，输入文件类型组名称和描述，文件类型的输入框输入各种类型的后缀名，如“*.mp3”或者“mp3”等。



位置对象组

位置对象组是用于通过IP段或VLAN类型划分不同位置。可以被权限管理、流控策略的章节引用。管理员可对该位置对象组进行新增、删除、导入/导出和搜索操作。

点击<新增>弹出位置对象组页面，输入名称和描述，位置类别可选IP段和VLAN。IP组：可选择具体的IP组，也可以输入IP范围，一行一个IP或者IP段。VLAN：可以输入VLAN ID，一行一个。

位置对象支持导入/导出。导出格式为inf格式。位置对象支持根据具体IP搜索，是否存在于此位置对象中。当搜索IP时，会将所在IP地址段也显示出来。比如：位置对象A为 2.2.2.2-5.5.5.5，当搜索IP为3.3.3.3时，也会把位置对象A显示出来。

说明：

1.一个用户只能属于一个位置，记录日志时会记录用户的位置。

2.位置对象间不能重复，同类型间可以界面上限制不能重复，但不同类型间没法限制。比如一个VLAN所包含的IP可能包含在一个IP段定义的位置里。因此，不同类型的对象位置存在重复时，按IP > VLAN 的顺序识别；最大支持1000个位置对象。

网络配置

网络配置的功能包括部署模式、网口配置、DHCP、高可用性、路由、高级配置。

可以配置部署模式和设置基础网络参数等信息。

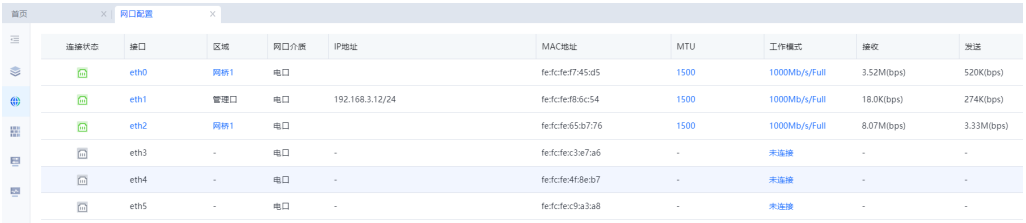
部署模式

全网行为管理的部署模式主要有三种，分别为：路由模式、网桥模式、旁路模式、单臂模式。当需要模式切

换的时候，会恢复到默认配置，建议切换之前备份原有的配置。具体部署操作指导请参考安装部署章节。

网口配置

在[系统管理/网络配置/网口配置]，页面显示网口连接状态、物理网口名、逻辑区域、网口介质、IP地址、MAC地址等信息。在网口配置目录下仅能修改已定义的网口的配置，而不能修改网口的定义。



连接状态：显示该网口的连接状态和MTU，其中连接状态显示表示连接，显示表示未连接。

接口：显示设备上的物理网口名。

区域：显示该接口所属的逻辑区域。

• LAN口是作为内网口使用，需要将LAN口接到内网方向。

• WAN口是作外网口使用，需要将WAN口接到外网方向。当设备以路由模式部署时，需要申请多线路授权
。

• DMZ口是作设备管理口使用。和LAN口一样DMZ口也是属于内网口，用户可以在DMZ口连接内网重要的服务器，从而使用全网行为管理设备的防火墙设置功能控制LAN口区内网用户的访问权限，保证服务器的安全。

网口介质：显示该接口的类型，设备支持的类型为：电口和光口。

IP地址：显示该网口配置的IP地址。

MAC地址：显示该网口的物理网卡的地址。

MTU：显示该网口的MTU信息，可配置MTU，MTU范围：700~1800，IPV6下至少要配置1280，否则IPV6地址会被清掉。

工作模式：显示该网口的物理网卡的工作模式，主要支持全双工、半双工模式，且支持自动协商和手动协商
。

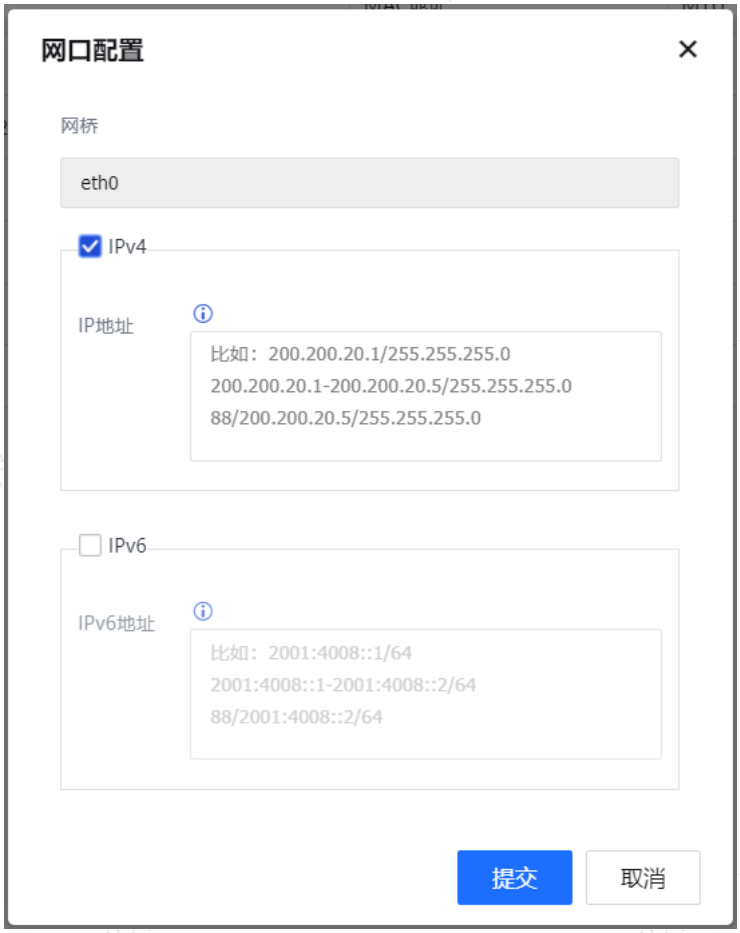
接收：显示该网口接收速率。

发送：显示该网口发送速率。

拨号日志：显示该网口拨号日志信息。

配置LAN口方法

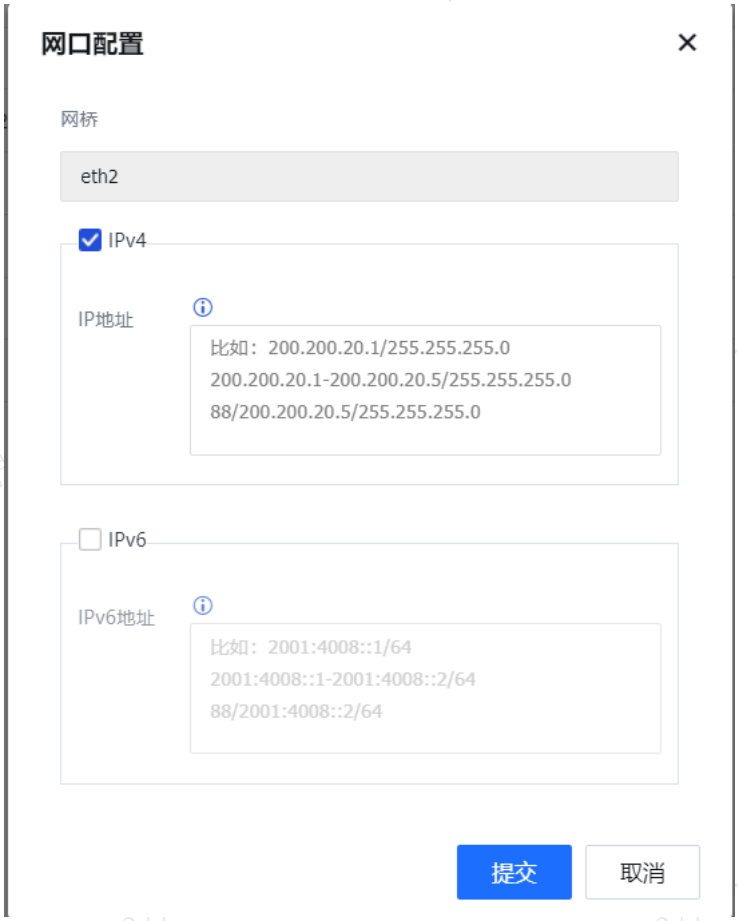
配置LAN口区网口eth0，点击<ETH0>弹出LAN口配置界面。



网口支持配置IPV4和IPV6地址。若接口启用VLAN，则在输入框中分别填写各个VLAN的ID及IP，此IP是分配给设备的某VLAN的空闲IP，如局域网中有VLAN 2，且VLAN 2的网段为10.10.0.0/255.255.0.0，假设10.10.0.1这个IP在内网没有被使用，则在VLAN地址列表中填写2/10.10.0.1/255.255.0.0。其他的VLAN信息依此类推，一行一个添加进去。可用于兼容VLAN（802.1Q）下的网络环境。

配置WAN口方法

配置WAN口区网口eth2，点击<eth2>弹出WAN口配置界面。



手动配置： IP地址可以配置为运营商来分配的固定IP，也可以选择自动获取运营商的IP，具体情况请咨询运营商。

PPPOE拨号：上网线路为ADSL拨号，用户名和密码为运营商（如电信，联通等）提供的账号和密码。

高级配置：配置拨号线路的拨号属性，建议握手时间为20，超时时间设置为80，最大超时次数设置为3，也可以根据其他需求进行设置。

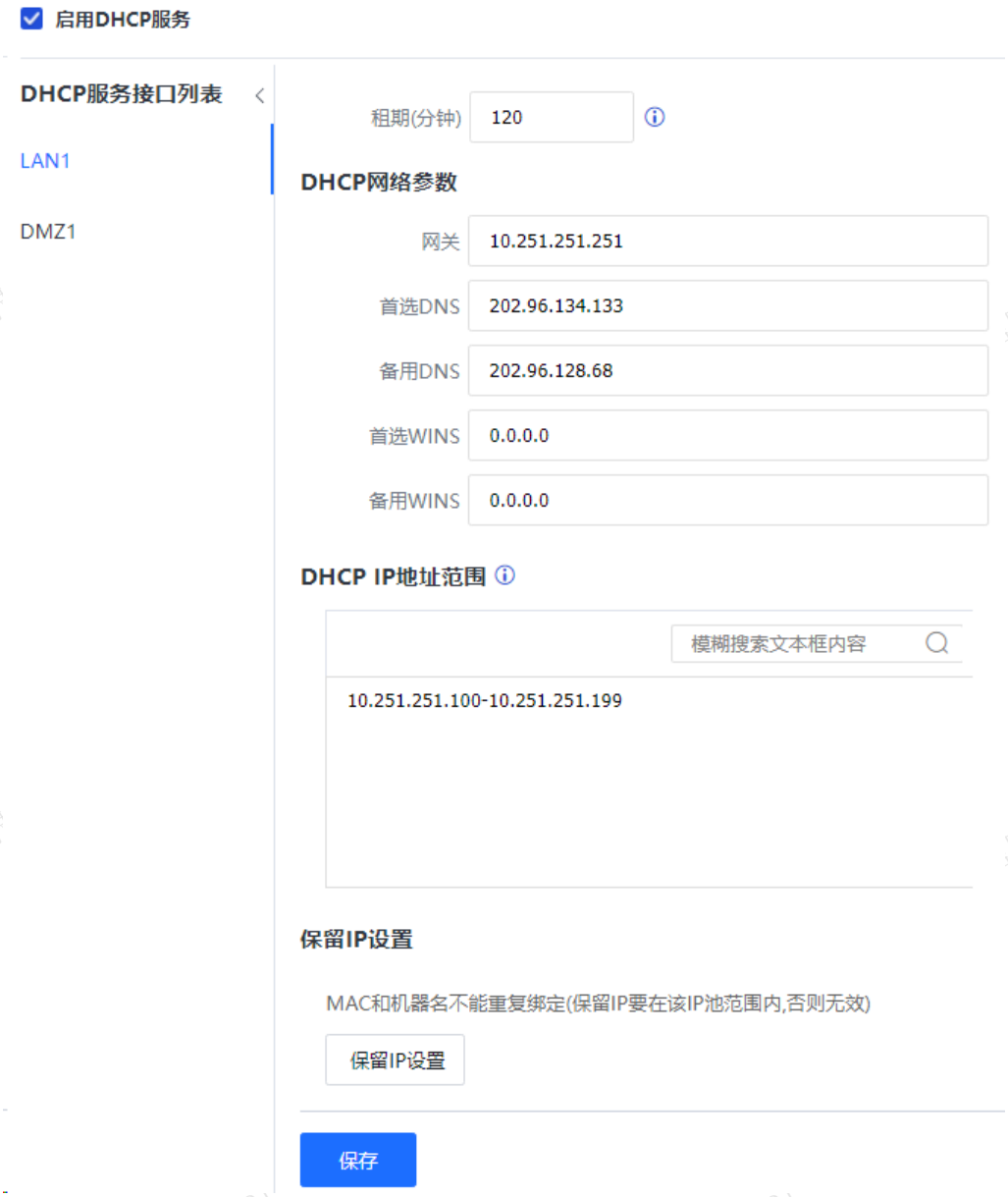
线路属性配置：配置实际链路的上下行带宽大小。

DHCP运行状态

DHCP运行状态是用于查看DHCP的分配情况，前置条件是需要先在[系统管理/网络配置/DHCP]，去启用DHCP服务，对LAN口和WAN口所接的电脑进行DHCP自动分配IP的相关设置后会显示相关信息。

DHCP

DHCP服务用于给内网终端自动分配IP地址，该服务只在路由模式的情况下可用。通过DHCP服务对LAN口和DMZ口两个内网口的终端自动分配IP时，需要分别设置两个网口的DHCP服务，且勾选[启用DHCP服务]后才会生效。



租期（分钟）：设置IP地址分配的租期，设置范围为1-7200分钟。

DHCP网络参数：设置DHCP自动分配的网关地址、DNS地址、WINS地址。

DHCP IP地址范围：设置地址分配的IP地址。

保留IP设置：MAC和机器名不能重复绑定(保留IP要在该IP池范围内，且流量是经过AC设备，否则无效)。

点击<保留IP地址>会跳转到保留IP设置页面，点击<添加>当输入当前跟AC匹配的IP地址，点击<确定>提交成功。

点击<获取MAC信息><获取机器名>设备会自动获取该IP地址目前的MAC和机器名称，然后将IP\MAC\机器名绑定。

获取到的信息如下所示。

光口bypass设置

高可用性

高可用性包括主备模式和主主模式两个功能。

• **主备模式**：是指相同的两台设备通过指定的以太网口（被称为HA口）通信互联，设备通过通信网口同步配置信息和当前会话等信息，设备分为一台主设备和一台备份设备，主设备处于活动状态处理请求并转发网络流量，同时将配置等信息同步到备份设备，当主机宕机或者发生网络故障时自动切换到备机工作。一般用于用户环境有主备两条线路的情况下，两台设备分别接主备两条线路，当主线路断开时备份线路启用，备份设备也会启用，并保持和主设备完全一致的配置，确保业务不会中断。

• **主主模式**：是指多台设备通过指定的以太网口（被称为HA口）通信互联，设备通过通信网口同步配置和用户在线状态等信息，此时多台设备是同时工作。实现在类似VRRP环境下某条线路断掉无缝切换到另一条线路时，全网行为管理设备可以正常工作，并实现策略和用户状态的一致性。

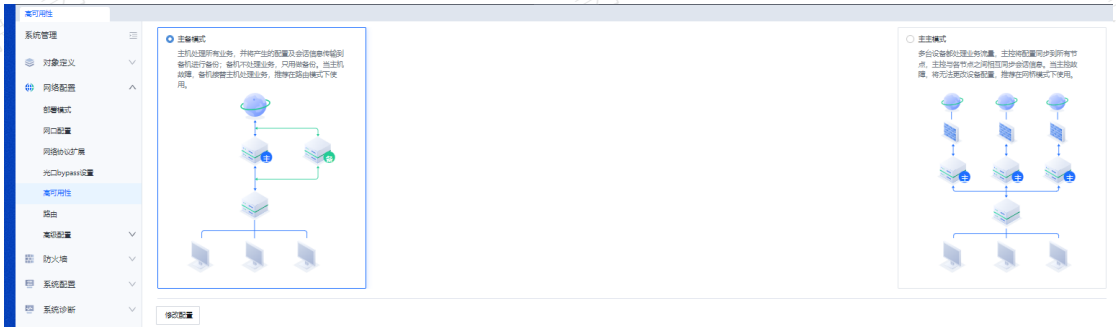
两者的共同点都是保证网络的稳定性，确保业务不被中断。两者的区别为主主模式是多台设备同时工作，同时在线；主备模式是两台设备互为主备，只有一台设备是工作在线的。主主和主备的使用要视环境而定。

主备模式

主备模式是指路由模式部署的两台设备通过心跳检测，实现热备份（保持心跳和配置同步）。正常情况下，只有主设备工作，如果主设备故障，则自动切换到备设备，备设备接替主设备工作。从而保证客户的业务不受影响，网络不中断。

主备模式只有一台主设备处于正常工作状态，另一台备机设备处于监听状态。

步骤1.在[系统管理/网络配置/高可用性]，选择主备模式。



步骤2.点击<修改配置>，跳转到更改高可用性模式页面，并设置相关的选项。

设备标识：用于设置当前设备标识，方便区分主备两台设备；

选举主机优先级：用于设置两台设备的优先级高低，两个设备同时开启高可用性，优先级为高的设备优先成为主机，优先级为低的设备为备机。目的是防止上架时两台设备同时启动备机先于主机启动，使得备机成为主机，导致上架异常。

步骤3.点击<基本配置>，填写相关参数，参数说明如下：

HA口主备模式下，可以设置两组HA口，主HA口和备HA口，主HA口是必填选项，备HA口为可填选项，HA口的网络配置不会同步。

共享密钥：配置的密钥用于校验主备设备之间的通讯，主备机的密钥需要保持一致，否则无法建立连接。主备状态建立成功后会以明文的方式显示。

监测网口组：配置需要监控的业务网口组，设备未启用的接口不需要监控。网口组内的网口是互为备份状态，只有同一个网口组内所有网口同时故障才会使该网口组进入故障状态，设备主备状态才会切换。

告警选项：告警选项可以配置当发生切换时，是否发送告警邮件。点击<配置告警选项>跳转到告警配置页面，勾选高可用性警告；详细配置参考告警选项章节。

说明：

手动更改模式也会触发告警。

点击<检测方式>，配置相关参数，如下图所示。

心跳超时时间：主备心跳超时时间设置,当心跳超时后备机会开始工作。

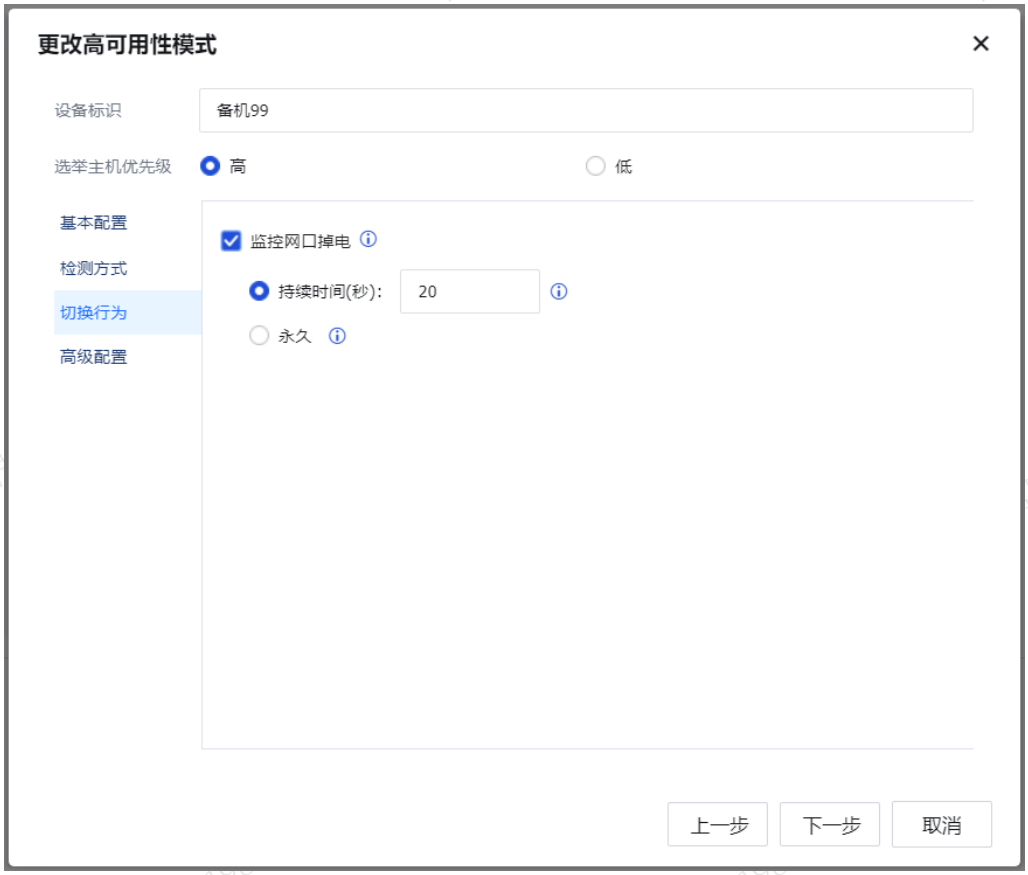
备机异常时主机避免进入故障状态：包括ARP探测和ICMP探测，当备机设备已经是故障状态是，如果当前设备只出现ARP探测故障或者是ICMP探测故障仍然保持主机状态正常工作。

ARP探测：主要是探测设备的上联或者下联设备的地址，只要有一个探测不通就进入ARP探测故障。ARP探测可以设置探测超时时间，探测故障恢复时间以及探测间隔。

ICMP探测：用于探测在[探测IP]栏中填写的主机IP或者域名的连通性，探测IP/域名可以支持填写多个，只有在所有IP或者域名探测都不通的时候才进入ICMP探测故障。ICMP探测可以设置探测超时时间，故障恢复时间以及探测间隔。

步骤4.点击<切换行为>，配置相关参数，如下图所示。

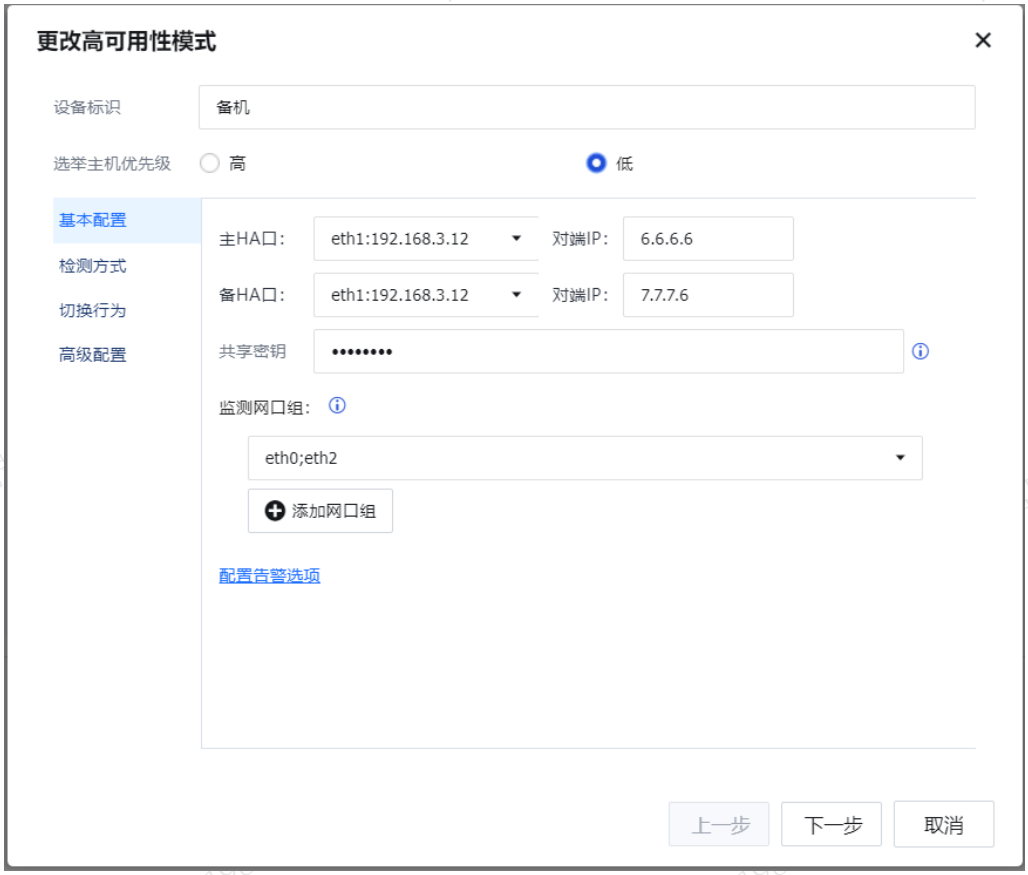
监控网口掉电：默认不勾选，在设备进入备机状态时，停用监控网口组内所有网口，用于通知上下联设备进行快速联动切换，切换行为一般适用于上下联设备监测网口掉电才会联动切换的场景。



步骤5.点击<高级配置>。勾选伴随升级，不拆主备完成两台设备版本升级。适用于通过web在线升级或BBC下发升级软件版本。

步骤6.点击<提交>，主机完成配置。

步骤7.配置备机。设备角色选择备机后，配置方法同主机，注意：备机的优先级不能和主机一样，备机的HA口填写主机地址。其中检测方式切换行为参考主机配置。



步骤8.主备设备上架

• 主机和备机上架并固定（通过耳片，托盘或导轨固定）。

• 按照实际规划拓扑接线。

• 主机先加电开机，等待主机成功启动后（alarm灯熄灭，控制台可以正常登录则成功启动），备机加电开机。

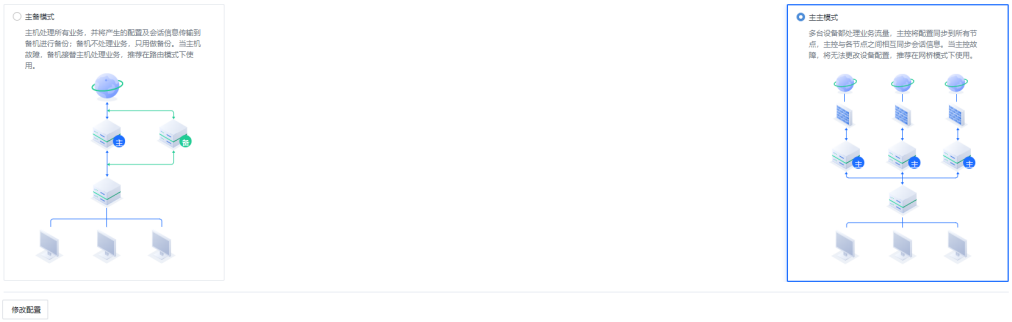
• 观察主机和备机的HA灯的状态，正常应该是主机Ha灯常亮，备机HA灯有规律的闪烁。(主要针对软件平台)

步骤9.正常工作后，主机的配置会通过HA口同步到备机，主机和备机建立成功之后，状态如下图--未找到此图。

主主模式

主主模式一般应用于内网VRRP环境，内网设备做热备的同时也做负载。架上设备后不会影响用户原有网络的工作及切换。多台设备都处理业务流量，主控将配置同步到所有节点，主控与各节点之间相互同步配置和在线用户。当主控故障，将无法更改设备配置，推荐在网桥模式下使用。

步骤1.在[系统管理/网络配置/高可用]，选择主主模式。



步骤2.点击<开始配置>跳转到高可用性模式配置页面，选择置主控模式。

设备标识：用于设置当前设备标识，方便区分的各台设备。

设备角色：用于选择主控或节点，如果是主控，只需要配置共享密钥。如果是节点，则需要输入主控IP和主控的密钥。

共享密钥：配置主控和节点连接的密钥，需要和节点保持一致。

告警选项：有设备离线时发送告警邮件，需配置告警邮件。

步骤3.另一台设备的设备角色选择节点模式。

主机地址：填写主控设备的地址。

共享密钥：主控和节点连接的密钥，需要和主控保持一致。

步骤4.配置完成，主主模式建立成功后，主控和节点界面分别显示如下图。

步骤5.主控可以同步配置，点击<开始同步>，此时设备会发送同步信号。进行设备的配置同步和信息同步。会显示所有节点状态，名称为“在线节点”，显示所有在线的节点。

注意事项：

1. 主备模式下，可以使用DMZ口或其他未配置的网口做心跳口，HA(心跳口)口的网络配置将不会同步。如果使用DMZ口作为心跳口，则DMZ口也不会同步网络配置；
2. 主主模式在线用户状态时实时同步的，当一台设备上有新的用户通过认证，则会立即同步到其他的设备。注意不需要认证的用户在线状态是不会同步的；
3. 主主模式下可不配置心跳线，只要节点能够和主控的IP地址通信即可，也可直接使用主控的网桥IP进行通信；
4. 网桥模式下只支持主主模式，不支持主备模式；路由模式下主主和主备都支持；
5. 网桥主主部署时，业务是否切换由下联交换机决定。如果网桥是一对bypass口组成，那么设备宕机则会进入bypass状态，此时网络仍然是通的，导致交换机检测不到上行链路down不会进行切换。若要实现主控设备宕机切换业务，建议网桥不接一对bypass口。

各种模式下高可用支持情况：

模块	子模块	路由模式	网桥模式	旁路模式	单臂模式
高可用性	主主模式	Y	Y	Y	N
	主备模式	Y	N	Y	Y

设备掉线、在线，HA灯具体状态显示如下：

	主备		主主	
模块	主机	备机	主控	节点
掉线	灭	灭	灭	灭
连接状态	亮（绿色）	1HZ闪	亮（绿色）	1HZ闪

如果主机/主控掉线，则会常亮（异常状态）。

路由

路由配置包括IPv4静态路由、IPv6静态路由、默认路由、OSPF动态路由，当设备本身需要和不同网段 IP通信时，需要通过路由实现数据转发。

静态路由

当使用设备在路由模式部署时，设备的LAN口IP是192.168.1.12/255.255.255.0，内网电脑的网段是192.168.2.0/255.255.255.0，内网的电话和设备之间接了三层交换机，当内网的电脑上网，上网的数据会经过三层交换机转发给设备，但是设备在转发数据给内网电脑时，因为是不同网段的IP，设备不知道将数据交到哪里，导致内网用户上不了网，此时需要设置静态路由，将内网网段的数据交给三层交换机，由三层交换机实现转发。

点击<新增>则弹出IPV4静态路由页面。

目的IP地址：需要到达的目标网段。

子网掩码：目标网络对应的子网掩码。

下一跳IP地址：达到目标网络的下一跳地址，但是不能填写设备的网口IP。

接口：从设备那个接口转发。

点击<查看系统路由>，将显示所有的系统路由，可查看IPv4路由和IPv6路由。

默认路由

当用户流量未匹配到的DNS代理或者负载策略时才会匹配默认路由，默认路由的优先级是最低的。

优先级说明：直连路由>静态路由>动态路由>DNS代理[重定向至线路]>优先负载策略>默认负载策略>默认路由。

链路故障检测：可以看到当前线路状态、线路、网口、检测方法等信息。

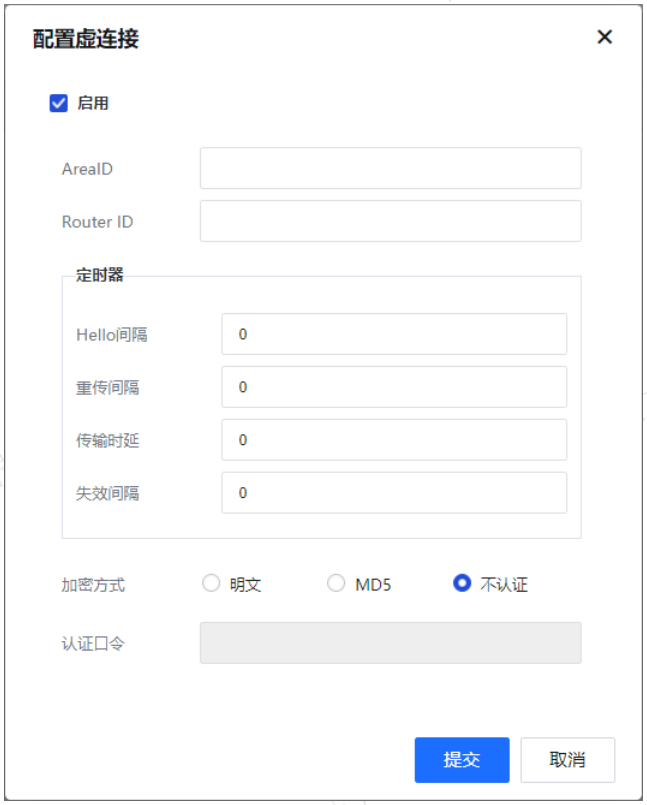
OSPF动态路由

全网行为管理AC可以设置并开启OSPF动态路由协议，包括网络配置、接口配置、参数配置、信息显示、调试选项等内容。设备支持IPv4的OSPF。

勾选启用OSPF，启用OSPF功能，会出现“确定开启OSPF”提示信息。

点击<是>，保存配置即可开启OSPF功能。

配置虚连接：当AC设备所在的区域与OSPF的骨干区域不相邻的时候，需要启用和配置虚连接。



勾选启用，开启虚连接。

Area ID：填写骨干区域ID。

Router ID：填写建立虚连接的对端路由器ID，指明与哪一台路由器建立虚连接。

定时器：设置hello包间隔，重传间隔，传输时延，失效间隔，单位是秒。

hello间隔：Hello报文的重发间隔时间，默认值是10s。

重传间隔：与接口相邻的连接状态报文重发时间，默认值是10s。

传输时延：传输一个链路状态更新数据包的估计时间，默认值是5s。

失效间隔：如果超过失效间隔时间还未收到Hello报文，则认为该OSPF邻居不可达，一般设置为hello间隔的4倍，默认值是40s。

加密方式：设置报文发送的加密方式，可以选择明文、MD5。默认是不认证。

认证口令：报文加密使用的口令。

点击<高级配置>，可进行路由重发布和NBMA邻居配置。可通过鼠标点击感叹号提示进行选择。

其中路由重发布包括重发布静态路由、重发布直连路由、重发布默认路由，有E1和E2可选择。

1. 网络配置

网络配置可设置设备需要发布的网段。根据需求填写运行网段和Area ID。

运行网段：设置需要发布的网段地址，填写格式为：IP/掩码。

Area ID：设置将该网段引入到哪个区域，一般填写骨干区域的ID。

2. 接口配置

接口配置显示设备在[OSPF/网络配置]中发布的网段对应的接口信息。如果在[OSPF/网络配置]下新增了如下网段。

自动生成的接口配置如下所示。

点击接口名称，出现如下页面。

接口名称：OSPF/网络配置中发布的网段对应的接口名称。

网络类型：可以选择广播、非广播多路访问、点到多点、点到点四种类型。

接口IP：接口IP地址。

被动接口：被动接口不发送OSPF链路状态，配置为被动接口后，直连路由可以发布，但接口的OSPF报文将会被阻塞，邻居无法建立。被动接口默认选“否”。

认证方式：可以选择明文，MD5，不认证，默认是明文认证。

认证口令：设置明文或MD5认证方式的口令。

接口开销：指定从某条链路发送报文的开销。接口开销会影响到LSA的Metric，直接影响OSPF的选路结果，范围为1-65535，默认值为1。

邻居老化时间（s）：默认失效时间为40s。

发送报文间隔时间（s）：Hello报文的间隔时间，默认为10s。

选举优先级：优先级为0的路由器不会被选举成DR或者BDR。DR由本网段路由器通过Hello报文共同选举，设备将自己选出的DR写入Hello报文中，发给网段上其他路由器。当同一网段的两台路由器都宣布自己是DR时，优先级高的胜出；如果优先级也相同，Router ID大的设备胜出。选举优先级默认值是1。

重传时间间隔（s）：缺省情况下，相邻路由重传LSA的时间间隔值为5s。

启用DD报文MTU不匹配检测：运行OSPF的设备在进行数据库同步时，使用DD报文描述自己的LSDB。默认情况下，接口发送DD报文时不填充MTU值，即DD报文中MTU值为0。

3. 参数设置

Router ID：设置AC设备的Router ID。

域内优先级：域内的LSA在计算后输出到路由表时，所携带的优先级(cisco设备中称为管理距离AD)，默认值为10。只支持OSPFv2。

域间优先级：域间LSA计算后输出到路由表中的优先级，默认值为110。只支持OSPFv2。

外部优先级：外部路由经过SPF计算后，输出到路由表时所赋予的优先级，默认值为150。只支持OSPFv2。

SPF计算间隔：当链路状态数据库LSDB发生变化时，需要重新计算最短路径，默认值是5s。只支持OSPFv2。

路由重发布设置：包括需要将直连路由，静态路由、默认路由引入OSPF路由中作为外部路由信息，并可设置路由引入后的metric值。

默认度量值：默认引入路由的跳数，在引入路由时，如果不分别指定各类型路由的metric 参数，则使用该度量值作为路由引入后的跳数。度量值默认值是20。

路由重发布配置中的所有度量值都只对OSPFv2有效。

4. 信息显示

通过信息显示可以查看OSPF链路信息、OSPF路由信息、OSPF邻接关系、OSPF接口信息。其中OSPF路由信息是用来查看OSPF路由信息。

OSPF链路信息

字段名称	字段说明
Type	LSA的type
Router ID	LSA所在的Router ID。*代表设备自己产生的LSA。
Adv Router	表示由哪个设备通告的这条LSA给本设备。
Seq	这条LSA的序号。
Age	表示收到该LSA已有多长时间。超时时间到了之后，该LSA将被老化。
Opt	表示Hello报文中携带的选项信息。如果邻居与设备本身的option字段一致，可以拒绝接收该邻居的消息。
Cksum	LSA的校验和。
Len	LSA的长度。

OSPF邻接关系

字段名称	字段说明
Neighbor ID	邻接路由器的路由器ID。
Pri	邻接路由器的优先级。
State	邻接路由器的功能状态。

Dead Time	如果邻居不发Hello报文，显示还有多长时间该路由器状态变为DEAD。
Address	邻居与本设备相连接口的 IP地址。当OSPF信息包被传输到邻居，此地址将是下一跳IP地址。OSPF_VL1是虚连接标识。
Interface	邻居与本设备相连的接口。

OSPF接口信息

字段名称	字段说明
Interface	接口名称。
IP	接口的IP地址。
Area	该接口所属区域。
State	该接口的角色。
DR	该区域的DR地址。
BDR	该区域的候选BDR地址。

调试选项

• 开启OSPF调试：**能调试显示事件、显示接口状态、显示邻居状态、链路状态广播、显示数据包、zebra调试信息。开启OSPF调试功能可能会对性能存在影响。**

• 清屏：**清空当前调试的信息。**

• 立即刷新：**刷新当前的信息。**

• 下载调试日志：**下载调试信息的日志。**

高级配置

高级配置包括HOSTS、GRE隧道、WAN口开放端口。

HOSTS

HOSTS用于定义设备内置的host表，以解决内网用户需要通过域名或机器名来访问内网资源的问题。可以定义“域名”或“机器名”对应的host主机IP。在[系统管理/网络配置/高级配置]，用户可以新增Hosts，编辑和删除操作。

说明：

Host文件生效的条件：内网PC的DNS地址指向全网行为管理的LAN口地址。

GRE隧道

GRE隧道用于配置GRE隧道，可以支持GRE OVER IP、GRE OVER OSPF和GRE OVER IPSECVPN。

在[系统管理/网络配置/高级设置/GRE隧道]，点击<新增>打开GRE页面。

隧道别名：新增tunnel口的编号的别称，自定义。

IP地址：作为新增隧道的IP地址，该IP地址所在网段作为OSPF运行网段。

区域：出接口所在的区域，可以选择LAN区或WAN区。

源端地址：本端出接口实际公网路由源地址。

目的端地址：对端入接口实际公网路由目的地址。

GRE密钥：共享密钥，两端要一致。

点击<高级配置>：用于设置MTU值、报文检验和以及链路状态检测的设置。

MTU：用于可传输设定数据包的尺寸，该取值范围为：68-1476。

报文校验和：对GRE头和报文信息进行检验。数据发送根据GRE头和payload信息计算校验和，并讲包含校验和和报文发送给对端。接收方和接收的报文计算校验和，并与报文中的值相比较，如果不同则丢弃。

链路状态检测：开启后，将按照下述时间间隔时间定期检测链路状态，在超时后没有收到隧道对端的回应，则本端重新检测链路状态。当达到最大发送次数后扔没有收到对端的回应，则把对端接口的协议连接宕掉，直达再次收到对端的回忆才开启。

点击<提交>，完成GRE隧道设置。

WAN口开放端口

在设备的WAN口方向对外开放特定端口时，需要管理员确认需求和安全性再开放。为了提升网络安全，AC设备仅支持少量的对公网开放端口，默认情况除必须对WAN方向开放的端口，其余端口都不对外开放。

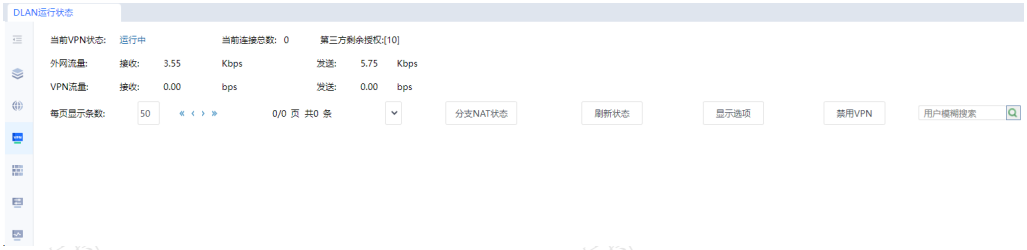
设备会提供四个常用端口的配置，状态默认关闭。需要启用时，点击状态按钮后，切换为绿色为启用状态，点击保存修改即可。也可以定义新的端口号，点击<添加>，输入端口号和描述信息。

VPN配置

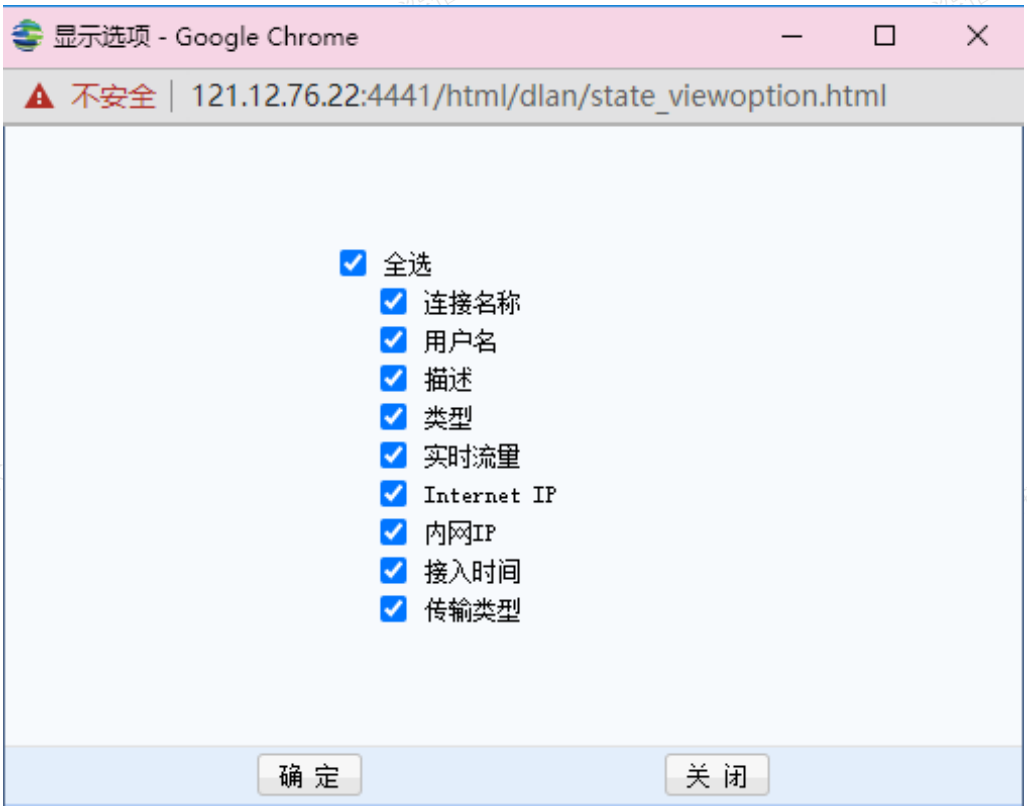
VPN配置包括DLAN运行状态、多线路配置、SDWAN智能选路、基本设置、用户管理、连接管理、虚拟IP池、本地子网列表、隧道间路由设置、第三方对接、通用设置、 证书管理、高级设置功能的配置。注意：VPN仅在路由模式下才会显示该功能。

DLAN运行状态

DLAN运行状态可以查看当前VPN连接和网络流量信息。用户可点击<分支NAT状态>查看NAT状态查询，<刷新状态>刷新当前页面，用于修改VPN状态后，<禁用VPN>禁用/启用VPN服务。



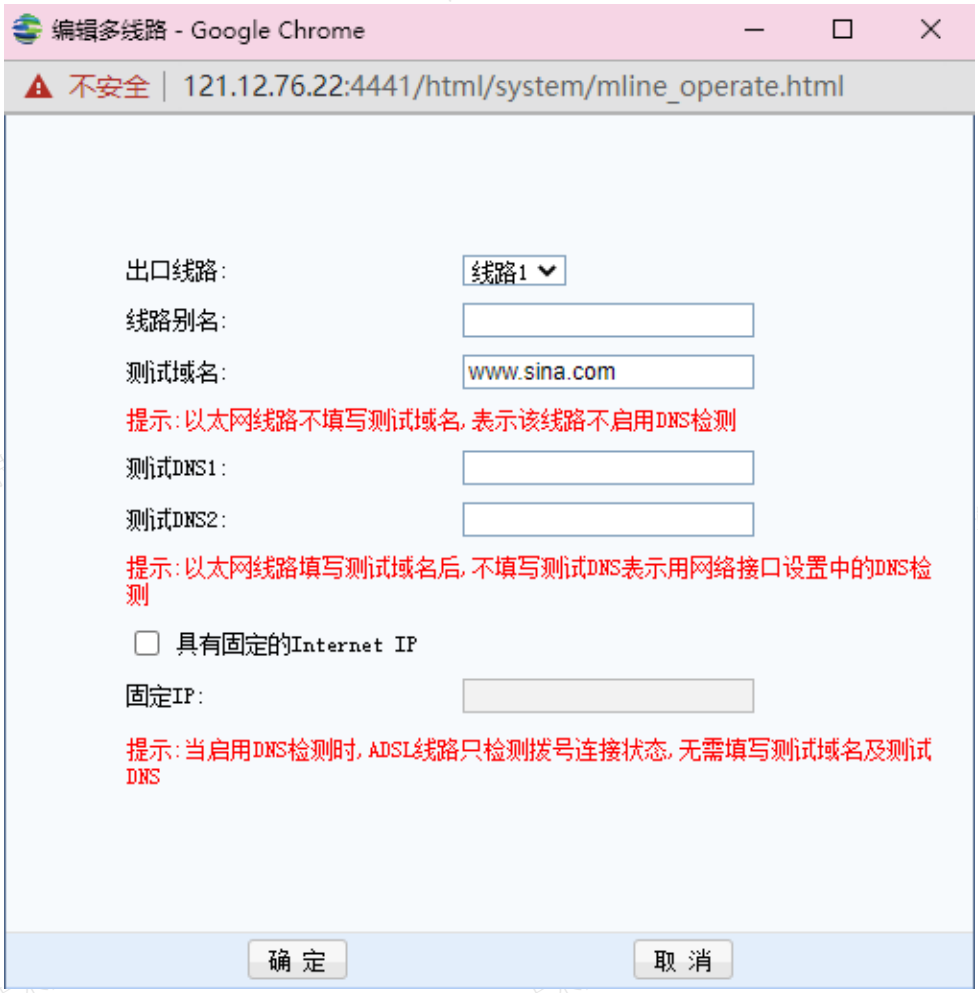
点击<显示选项>可显示列表信息，默认是全选。



多线路配置

在使用多条WAN口线路时，必须设置多线路设置属性，管理员能对线路的信息进行增加、删除、修改和刷新操作。

当设备为WAN口且启用多线路时，勾选启用多线路，然后进行多线路的添加，点击<新增>按钮，增加线路，配置如下图。



说明：

1．当线路类型为以太网方式时，必须填写[测试DNS]，且所填写的DNS地址必须为正常工作的公网DNS地址。如果为ADSL拨号线路等，则可不填。

2．这里的[带宽预设]项请根据线路的真实情况填写带宽参数。

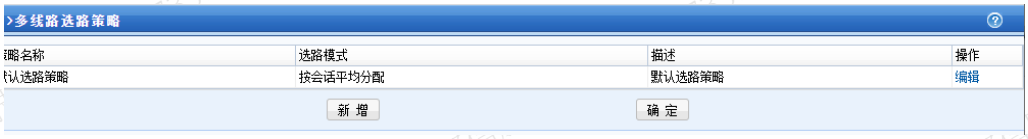
3．任何设置都必须点击<确定>按钮才能保存生效。

在多线路设置界面点<高级>按钮，出现多线路高级设置。

勾选[启用DNS检测]，可开启多线路状态检测功能。

[DNS检测时间(1-120)]：用于设置多线路状态检测功能检测DNS的间隔频率，在激活DNS检测时该设置才有效。

点击<多线路选路策略>跳转到多线路选路策略页面，在此页面可以定制多线路的选路策略，该页面有一个默认选路策略，管理员还能进行新增和编辑操作，详细操作，可点击<帮助提示>进行操作。



SDWAN智能选路

SDWAN智能选路功能是对以前的SANGFOR VPN多线路的升级，增加了按业务分类调度到指定链路和链路质量QOE识别，支持指定重要业务走指定线路，或者根据链路质量选择最优的线路。

SDWAN主要功能：

1. 根据内网服务来识别应用。
2. 使用该功能设备需要有多线路和分支机构才能生效。
3. 支持三种选路模式，对端如果没有选路，默认按wan1-wan1选路，否则按优先使用质量最好线路选路（若未配置线路标签，则按照wan1-wan1为同运营商处理）。

• 指定选路：**根据内网服务指定选择走某条线路。常用于视频会议业务，或者某些对线路有要求的业务。**

• 剩余带宽负载：**根据实时线路空闲的带宽比例去分配连接。常用于文件上传或者下载应用，对线路质量要求不高的业务。**

• 优先使用质量最好的线路：**根据线路的实时质量情况选择线路质量最好的那一条线路。常用于对线路质量要求较高的业务。**

4. 线路故障后，1s内切换线路，业务不会断开。
5. 流量管控策略的服务优先级功能（极高、高、中、低、极低五个等级），优先级越高的业务优先保证带宽，需要提前设置线路带宽，该功能才会生效。
6. 配置SDWAN智能选路前，先完成多线路设置。

默认一条“全局选路策略”不可以删除。

点击<新增SDWAN智能>选路策略，策略名称：用来定义策略的名称，可以自定义。内网服务：选择线路生效的内网服务。

指定线路

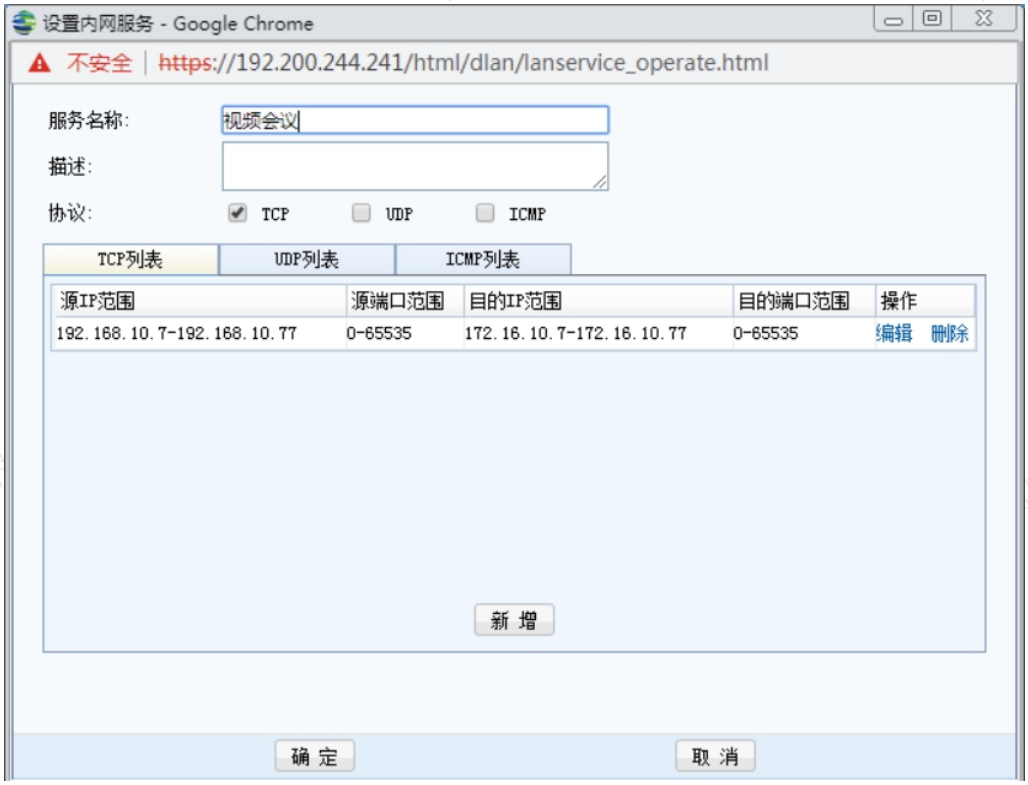
指定线路：优先使用排序靠前的线路，当排序靠前的线路故障或繁忙时，按序使用下一条线路。

举例：总部和分支有专线和VPN两条链路，希望视频会议流量走专线，其他业务流量走VPN。

假如线路一是互联网固定IP，线路二是专线，设备wan1和wan2分别对应线路一和线路二。

步骤1.总部分支建立VPN连接。

步骤2.在[高级配置/内网服务设置]新增视频会议服务。



步骤3.在[高级配置/内网服务设置]新增“其他流量走VPN”服务，服务选择所有服务。

步骤4.选路模式选择[指定线路]，线路选择线路一，服务选择其他流量走VPN服务。

步骤5.创建SDWAN策略“视频会议”，服务选择视频会议，选路模式选择[指定线路]，线路选择专线。

步骤6.确定“视频会议”这条SDWAN选路策略是在最上面的即可。

实现了分支通过VPN与总部开视频会议流量走专线，VPN隧道内其他流量走互联网线路，使视频会议流量得到保障。

说明

：

1. 优先同运营商的线路建立连接。

2. 当选用的线路全部中断或繁忙时，默认从剩下的线路中选用质量最优的。

多线路负载

1. 剩余带宽比例负载

总部和分支有两条VPN链路，希望分支访问总部的业务根据带宽剩余情况动态负载。

创建SDWAN策略，服务选择所有服务，选路模式选择[多线路负载]，负载线路将分支的两条选路都选择上，负载模式选择[剩余带宽比例]。

说明

：

1. 查看VPN详细连接信息显示的流速比配置带宽低，是因为过VPN会加密，数据包多了VPN头部字段。

2. 当前版本未在前台显示每条连接选路情况，工具无法控制每条TCP连接流速，所以在前台只能看到两条线路均跑满带宽。

3. 只支持多连接负载，不支持单连接负载。

---

2. 按链路质量选路

总部和分支有两条VPN链路，希望分支访问总部的业务根据链路质量情况进行选路。

创建SDWAN策略，服务选择所有服务，选路模式选择[多线路负载]，负载线路将分支的两条选路都选择上

，负载模式选择，负载模式选择[优先使用质量最好线路]。

说明：

1. 连接详细信息线路延时统计会有5ms以内误差；我们会把乱序包统计为丢包率，所以有时候在没有丢包的环境下会显示出丢包率数值，那可能是因为存在乱序包。

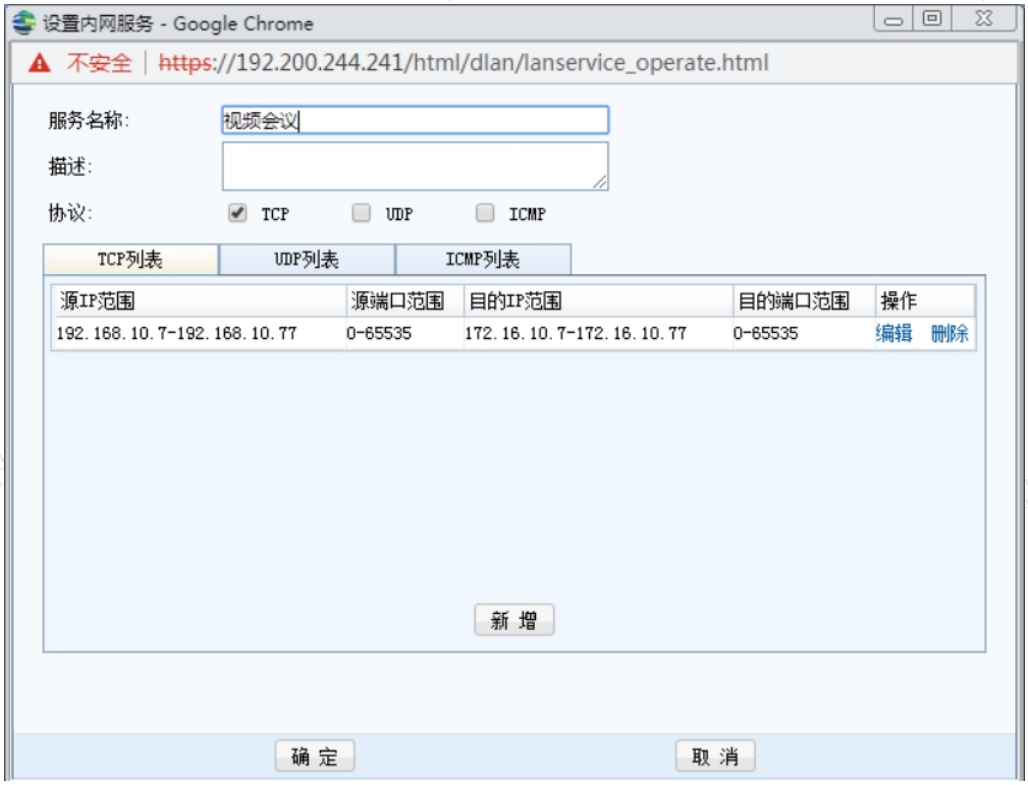
2. 当链路质量发生变化时，已有的连接信息不会重新选路，只有新建的连接会重新选路。

3. 服务优先级

在SDWAN选路看到有服务优先级，分为极高、高、中、低、极低五个级别。SDWAN通过服务优先级对数据做流量控制（QOS优先级）。

使用场景：总部和分支有电信、联通两条VPN链路，希望一般正常情况下分支访问总部的业务根据带宽剩余情况动态负载，当有视频会议流量时，电信线路优先保障视频会议的流量。

步骤1.在[VPN配置/高级配置/内网服务设置]新增视频会议服务。



步骤2.在[VPN配置/高级配置/内网服务设置]新增“其他流量走VPN”服务，选择所有服务。

步骤3.创建SDWAN策略“其他流量走VPN”，选择当前分支，服务选择所有服务，选路模式选择[多线路负载]，负载线路将分支的两条选路都选择上，负载模式选择[剩余带宽比例]，服务优先级选择[低]。

步骤4.创建SDWAN策略“其他流量走VPN”，选择当前分支，服务选择所有服务，选路模式选择[多线路负载]，负载线路将分支的两条选路都选择上，负载模式选择[剩余带宽比例]，服务优先级选择[低]。

步骤5.创建SDWAN策略“视频会议”，选择当前分支，服务选择视频会议，选路模式选择[指定线路]，线路选择[电信]，服务优先级选择[极高]。

基本设置

基本设置用于设置VPN连接所需的Web agent信息、共享密钥、VPN数据的MTU值、MSS值、VPN监听端口、广播组播设置。

[Web agent]指动态IP寻址文件在WEB服务器中的地址，包括主Web agent和备份Web agent地址。

如果是“动态寻址（总部非固定IP）”请填写“Web agent网页地址”（一般为以.php结尾的网页地址），填写完Web agent后可以点击测试按钮查看是否能够连通，如果总部是“固定IP”，请按照“IP地址：端口”的格式填写，如202.96.134.133:4009。

点击<修改密码>可以设置Web agent密码，为了防止非法用户盗用Web agent更新虚假IP地址。

共享密钥可以设置共享密钥，防止非法设备接入，设置完成之后可以点击，查看共享密钥>，该登录密钥即是指管理员密码。

说明：

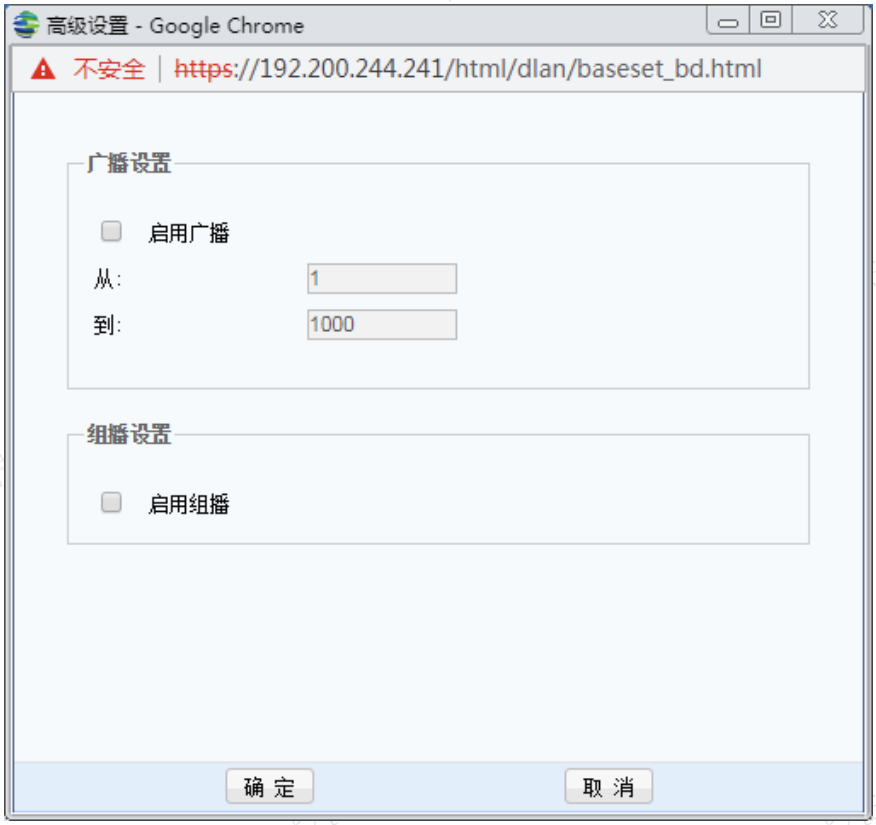
1．如果设置了[Web agent密码]，一旦遗失该密码则无法恢复，只能联系深信服科技用户服务中心重新生成一个不包含Web agent密码的文件并替换原有文件。

2．如果设置了[共享密钥]，则所有VPN网点必须设置相同的[共享密钥]才能相互连接通信。

3．如果是多线路且都是固定IP的情况下，可以采用“IP1#IP2:port”的方式来填写Web agent。

MTU值、修改MSS一般情况下请保留默认值，如需设置，请在深信服技术支持工程师的指导下修改。

点击<高级>，出现如下界面。



广播包设置：用来设置是否在VPN通道内传递广播包，并且只传递指定端口范围的广播包，尽可能避免VPN两边的广播风暴产生。如网上邻居、飞鸽传书等应用，均需要广播包的支持。

组播设置：用来设置是否在VPN隧道内传递组播包，某些视频应用可能需要组播包的支持。

点击<确定>，完成服务端的基本设置。

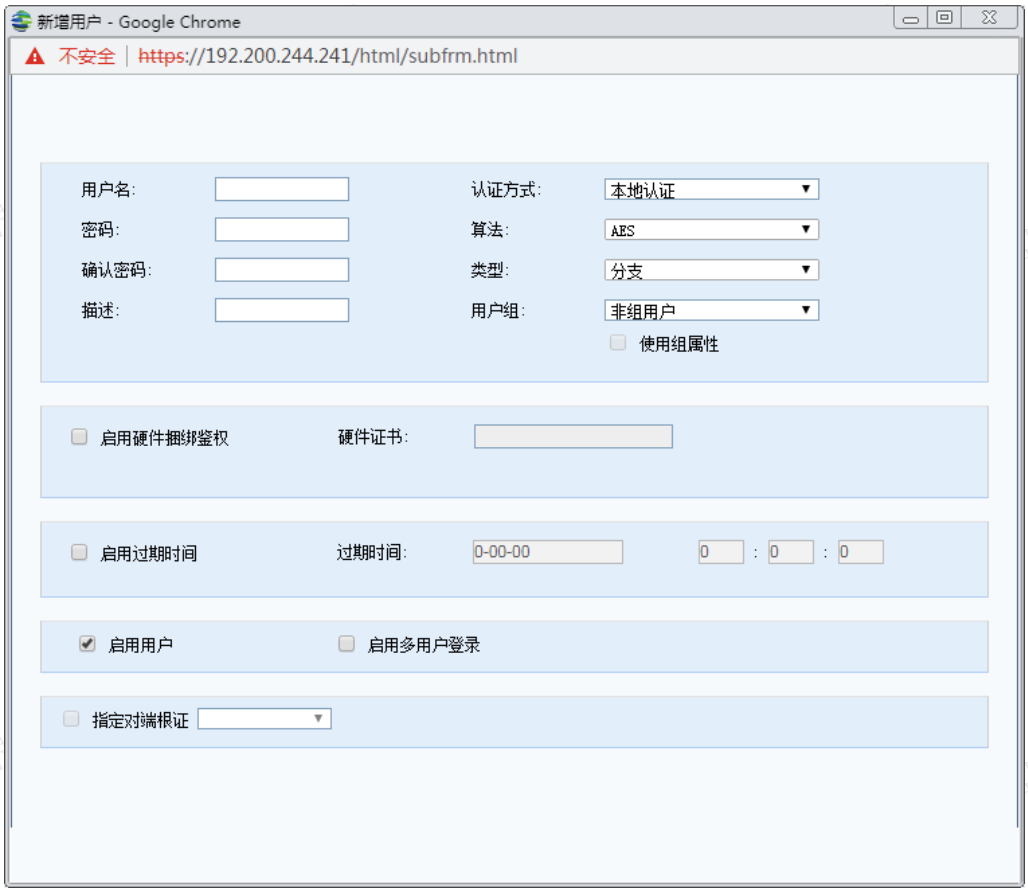
用户管理

用户管理用于管理VPN接入账号信息，设置允许接入VPN的用户账号、密码，是否启用硬件捆绑鉴权、是否启用虚拟IP、设置账号使用的加密算法、账号有效时间、账号的内网权限，对用户进行分组并设置组成员的公共属性等用户策略。页面如下。

点击<查询>点击可对输入的用户名/用户组进行查找，以便对查找出来的用户进行编辑操作。查找到的用户会用高亮显示，页面如下。

点击<高级查询>可对查询的用户增加一些过滤条件进行查找，支持勾选用户名模糊查询（不勾选模糊查询将完全匹配关键字，多个关键字请用英文逗号隔开），包括用户所属的用户组、组属性（不限/启用/禁用）、状态（不限/启用/禁用）等等。页面如下。

点击<新增用户>可依次设置接入账号的用户名、密码、描述、算法、类型等信息。



用户名：用于定义用户名称，如果认证方式选择是证书认证，此用户名必须与分支的证书的“颁发给”字段一样。

描述：对新增的用户进行备注描述，便于管理。

认证方式：用于设置用户认证类型，可选本地认证（即本地密码认证）、LDAP认证、Radius认证、证书认证。

说明
：

1．使用Radius认证和LDAP认证之前，请先在LDAP认证或Radius认证里设置好对应的认证服务器。

2．如果是缺省用户，认证方式不支持本地认证。

算法：可以选择包括DES、3DES、AES、SANGFOR_DES、AES192和AES256共6种算法。算法选择要两端一致。

类型：可以定义该用户是类型是分支。

使用组属性：用于对用户进行分组，如勾选[使用组属性]，则可激活选择[用户组]设置，选择将该用户加入到某一个用户组并使用这个组的公共属性。

说明
：

1．设置[使用组属性]前请先新增用户组。用户加入用户组后。

2．该用户的[加密算法]、[启用网上邻居]、[权限设置]、[高级]将无法单独设置。

启用硬件捆绑鉴权：用于设置基于硬件特性的证书认证，启用后请选择对应此用户的证书文件（*.id）。

启用过期时间：用于设置“接入账号”的过期时间。

启用用户：用于设置是否启用该用户。

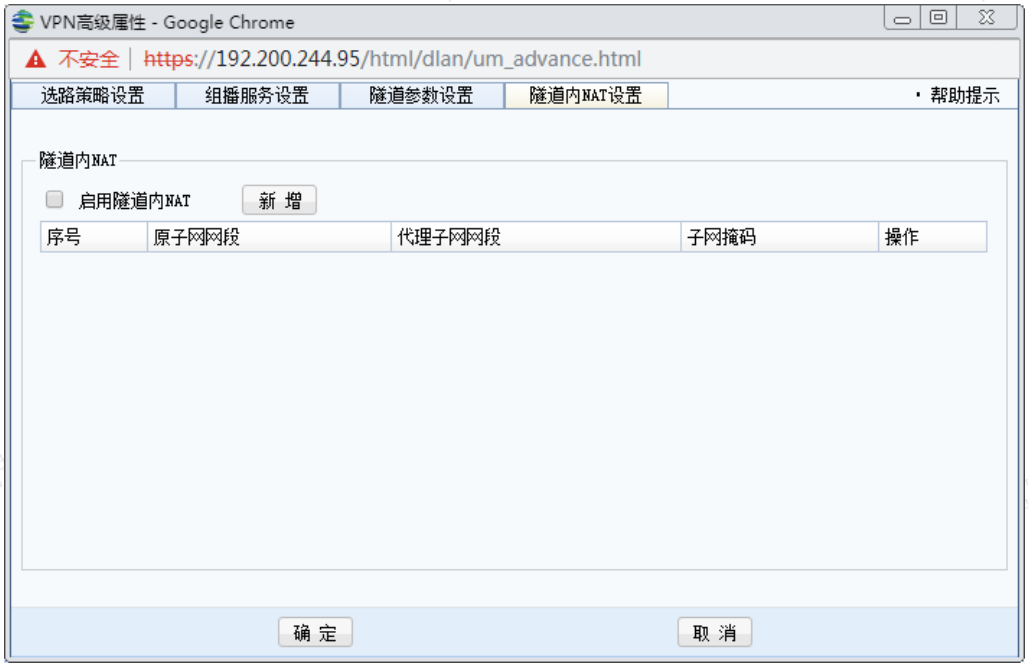
启用多用户登录：用于设置是否允许多个用户同时共用该账号登录VPN。

指定对端根证：当分支使用的证书与本端证书不是同一个CA中心颁发时，需要先将对端的CA根证导入到证书信息列表中，并在此处勾选“指定对端根证”选择对应的CA根证。

权限设置：用于设置用户接入VPN后的访问权限，即设置用户只能访问某些服务，默认不做限制。使用[权限设置]前，请先在[内网服务]处添加所需服务。添加方法请参考[内网服务设置]小节。

点击<高级>会跳转到高级设置页面，于设置用户接入VPN后的一些高级属性，包括选路策略设置、组播服务设置、隧道参数设置、隧道内NAT设置等。

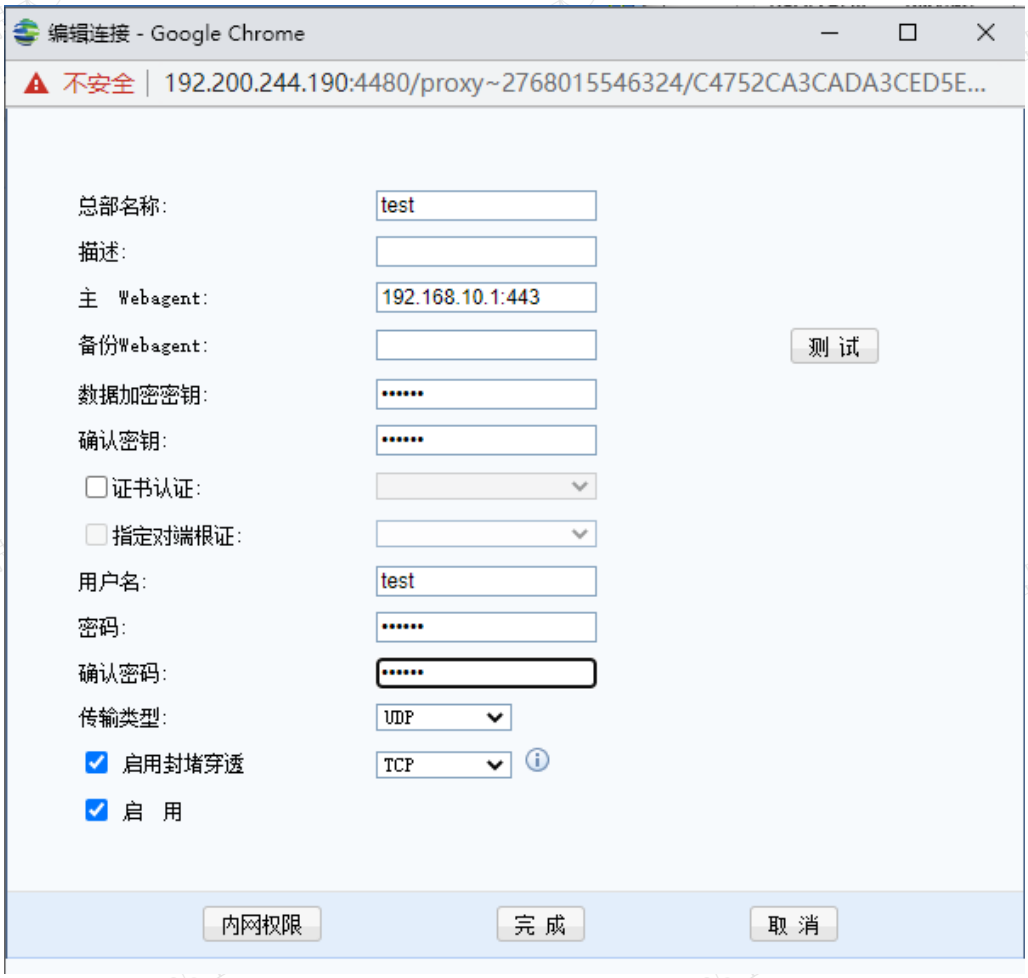
1. 选路策略设置是基于多条线路的连接状况，动态的在多条线路中选择最优线路进行传输，并且可以设置多条线路同时进行传输。
2. 组播服务设置主要是满足服务端和分支间有视频等需要组播协议支持的应用需求。
3. 隧道内参数设置主要是避免某个接入的分支VPN流量过大的问题。
4. 隧道内NAT设置主要是解决两个内网网段相同的分支同时接入到服务端时的地址冲突问题。



连接管理

连接管理可以实现多个网络节点的互联（组成“网状”网络），设备提供了对网络节点互联的自主管理和设置功能。连接管理只有此设备当分支需要连接其他总部设备时才启用，当本端是总部设备情况下不需要启用连接管理。

点击<新增>可以添加到总部的连接。



总部名称和描述：用于标记连接名称，可以任意填写。

主/备份Web agent：用于填写需要连接的总部的对应Web agent。

点击<测试>按钮可以测试Web agent是否工作正常，结果如下所示。

测试请求均是从本机发起的而不是设备发起的。如果Web agent是用域名形式，测试成功代表该网页存在，否则网页不存在。如果Web agent采用固定IP方式，则测试成功代表填写的IP：PORT格式正确。该测试成功并不代表VPN就一定能连接成功。

传输类型：可选“TCP”或“UDP”，用于决定传输VPN数据包的类型，默认为UDP模式。

数据加密密钥、用户名和密码：根据总部提供的接入账号信息来填写，如果勾选证书认证，则用户名自动获取证书中颁发给字段。

证书认证：如果总部选择的是证书认证，此处则勾选。

指定对端根证：当总部使用的证书与本端不是同一个CA颁发时，需要勾选此选项。

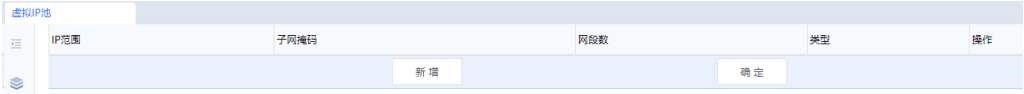
启用封堵穿透：可选“TCP”或“ESP”。

点击<内网权限>可以对VPN连接对端进行权限设置，即指定VPN连接对端只能访问本端的哪些服务。设置完以上信息后勾选[启用]选项即激活该连接。

最后点击<确定>按钮保存设置信息。

虚拟IP池

虚拟IP池可创建分支用户虚拟IP池。分支虚拟IP池中的虚拟IP段是提供给分支接入到总部时将分支的原网段替换成虚拟IP池中的一个网段，以解决当两个相同网段的分支同时接入到总部时的内网IP冲突问题。



点击<新增>，选择类型为[分支]，设定虚拟IP的开始IP、结束IP（点击计算可以自动计算出符合要求的结束I

P）、掩码和分支的网段数。

- 起始IP：**分支虚拟IP段的第一个IP地址。**
- 结束IP：**分支虚拟IP段的最后一个IP地址。**
- 计算：**自动计算虚拟IP段的最后一个IP地址。**
- 网段数：**需要多少个虚拟IP段。**
- 子网掩码：**虚拟IP段的子网掩码。与分支端子网掩码保持一致。**

设定分支虚拟IP段后，在[VPN信息设置/用户管理]里新建用户，用户类型选[分支]，然后在[高级/隧道内NAT设置]里配置需要转换的分支网段。

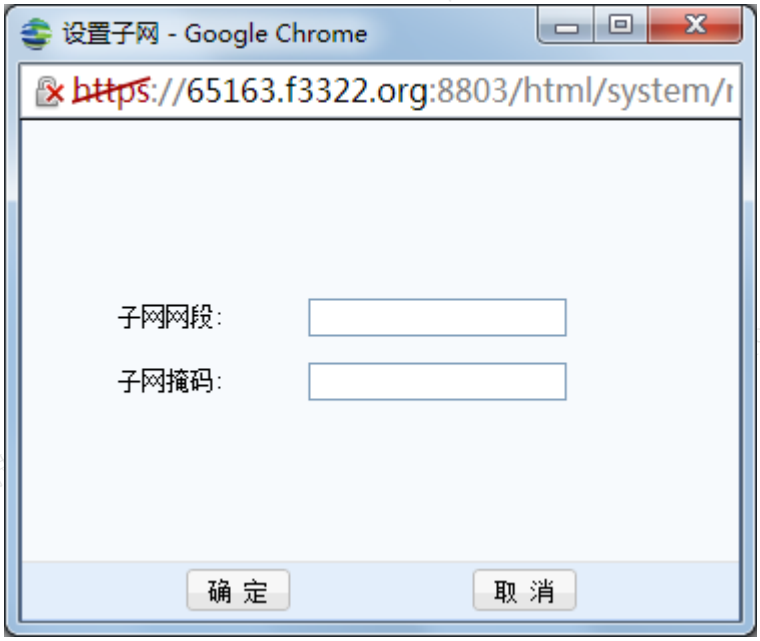
本地子网列表

本地子网列表用于硬件设备的内网有多个子网的情况下，VPN接入用户需要与总部内网的其它子网互访。

例如：部有两个子网（192.200.100.x、192.200.200.x），通过配置“本地子网列表”，可实现分支总部内网各网段相互访问。具体配置如下：

步骤1.在[本地子网列表]里配置需要互联的子网，页面如下。

步骤2.点击<新增>，添加子网网段和子网掩码。



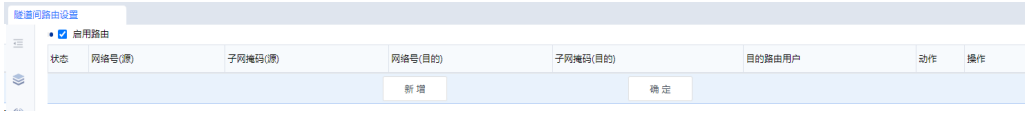
步骤3.[子网网段]和[子网掩码]：设置为本端内网非AC设备LAN/DMZ口直连网段的网络号和子网掩码。

步骤4.在[系统管理/网络配置/静态路由]中为需互联的子网设置可达的路由。

这里的[本地子网列表]仅相当于一种“声明”作用，在此定义的网段，都会被我们的VPN设备和软件客户端视为VPN网段，所有访问这些网段的数据包经过VPN设备或软件后，都会被封装到VPN隧道中传输。一般情况下，在本地子网列表里添加了子网网段，都需要配合静态路由来完成对多子网的访问。

隧道间路由设置

深信服设备提供了强大的VPN隧道间路由功能，通过设置隧道间路由，可轻松实现多个VPN（软/硬件）之间的互联，真正实现“网状”VPN网络。



例如：总部（“深圳”192.168.1.x/24）同时与分支（“上海”172.16.1.x/24）、（“广州”10.1.1.x/24）建立了VPN连接（分支“上海”、“广州”通过设置连接管理实现与总部互联），但“上海”与“广州”之间没有VPN连接，通过设置适当的“隧道间路由”规则，即可实现“上海”与“广州”之间的相互访问，具体配置如下：

步骤1.在分支“上海”的隧道间路由设置中勾选<启用路由>，点击<新增>，添加到“广州”的路由，页面如下。

- 网络号（源）：**设置源地址网络号，本例中应设置为172.16.1.0**。
- 子网掩码（源）：**设置源地址子网掩码，本例中应设置为255.255.255.0。**
- 网络号（目的）：**设置目的地址网络号，本例中应设置为10.1.1.0。**
- 子网掩码（目的）：**设置目的地址子网掩码，本例中应设置为255.255.255.0。**
- 目的路由用户：**设置路由指向的VPN连接用户。**
- 网络号（源）、网络号（目的）：**用于匹配数据的源IP地址、目的IP地址，当VPN隧道中传输的数据匹配设置时，则此路由设置生效，数据将被转发给相应的VPN设备。目的路由用户：可理解为“要将路由的数据发往哪一个VPN设备”，本例中分支“上海”在[连接管理]中设置了使用用户名“shanghai”与总部建立了VPN连接，因此以用户名“shanghai”标示将路由的数据发往总部。**

步骤2.在分支“广州”的隧道间路由设置中勾选<启用路由>，点击新增，添加到“上海”的路由，页面如下。

- 网络号（源）：**设置源地址网络号，本例中应设置为10.1.1.0。**
- 子网掩码（源）：**设置源地址子网掩码，本例中应设置为255.255.255.0。**
- 网络号（目的）：**设置目的地址网络号，本例中应设置为172.16.1.0。**
- 子网掩码（目的）：**设置目的地址子网掩码，本例中应设置为255.255.255.0。**
- 目的路由用户：**设置路由指向的VPN连接用户，本例中应设置为“guangzhou”。**

步骤3.隧道间路由还可用于设置将分支的上网数据全部发往总部，通过总部的公网出口上网，例如，在分支上海设置通过总部上网，页面如下。

• 网络号（源）：**设置源地址网络号，设置本端需要通过总部上网的网络号。**

• 子网掩码（源）：**设置源地址子网掩码，本例中应设置为255.255.255.0。**

• 目的路由用户：**设置路由指向的VPN连接用户，本例中应设置为上海。**

步骤4.勾选[通过目的路由用户上网]和[启用]，点击<确定>，保存设置。

步骤5.通过总部线路上网时，则必须在[系统管理/防火墙/NAT代理上网]中添加对VPN网段的代理规则。

第三方对接

深信服设备提供了与第三方VPN设备互联的功能，能与第三方的VPN设备建立标准IPSec VPN连接。管理员需要先把第一阶段的信息配置好才能进行第二阶段的配置，不能直接配置第二阶段。

第一阶段

第一阶段用于设置需要与深信服设备建立标准IPSec连接的对端VPN设备的相关信息。

点击<新增>，显示设备列表设置对话框，需要设置设备名称和描述.

线路出口：选择通过哪条出口线路与对端进行标准IPSEC VPN 互联。

设备地址类型：包括固定IP、动态IP以及动态域名三种。

• **选择“对端是固定IP”，则需要设置对端的固定IP地址以及预共享密钥；**

• **选择“对端是动态域名”，则需要设置动态域名以及预共享密钥；**

• **选择“对端是动态IP”，则仅需设置预共享密钥，选择该选项后仅能使用野蛮模式对接；**

作为备份设备：同一个设备支持备份隧道，如果有建立主备隧道，主隧道断开，数据包才会通过备份隧道发往对端。

如果配置时，误勾选了启动主动连接，设备会弹出提示框。

点击<高级>，则弹出高级设置对话框，界面如下。

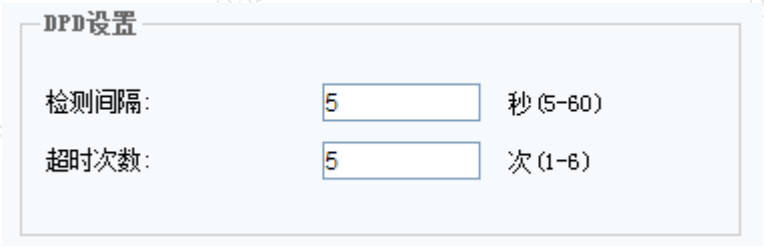
ISAKMP存活时间：用来设置第一阶段策略的生存期，只支持按秒计时。

重试次数：用来设置第一阶段协商时的重试次数。

支持模式：用来选择第一阶段协商所使用的模式，包括主模式和野蛮模式。

D-H群：用来设置协商双方的Differ-Hellman群，包括MODP768群（1）、MODP1024群（2）、MODP1536群（5）、MODP2048群（14）、MODP3072群（15）、MODP4096群（16）、MODP6144群（17）、MODP8192群（18）。

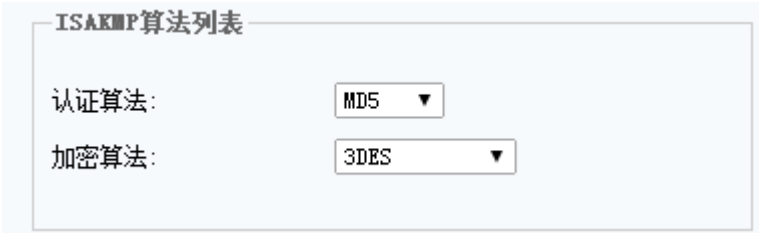
勾选<启用DPD>，启用死亡对等体检测功能，用于帮助VPN设备检测存在于隧道另一端的设备故障。



检测间隔：用于设置检测对端状态的时间间隔，设置范围5s-60s。

超时次数：用于设置检测到对端状态超时次数，设置范围1-6次。当达到超时次数，设备认为对端设备故障。

ISAKMP算法列表。



认证算法：用来选择第一阶段的认证算法，包括MD5、SHA-1、SHA2-256、SHA2-384、SHA2-512。

加密算法： 用来选择第一阶段的加密算法，包括DES、3DES、AES、SANGFOR_DES、AES192、AES256。

勾选启用选项，则此策略设置完成后立即生效。点击<确定>后保存并启用规则。

说明：

1．标准IPSec只支持路由模式部署，不支持网桥和单臂模式部署。

2．标准IPSec也不支持两端都配置对端为动态IP的环境。

3．加密算法如果选择 深信服的DES则要求双方都是深信服的设备。

第二阶段

第二阶段主要配置VPN的[入站策略]和[出站策略]，如下图。

管理员需要对入站策略和出战策略配置所用到的一样的参数进行统一说明。

表25出战策略和入站策略相关操作说明表

操作	功能说明
策略名称	可自定以策略名称
描述	简单描述该策略的作用
源IP类型	可选择单个IP或者子网+掩码
源IP地址	用来设置允许VPN对端访问本端的IP地址或IP地址段。
对端设备	用来选择对端设备，该设备在第一阶段中进行定义。
过期时间	可以设置该策略的过期时间，到了指定的时间则此策略失效。
启用策略	启用该策略，如果对端设备设置了PFS，则需同时勾上[启用密钥完美向前保密]。

其中入站策略和出战策略不同参数的说明：

入站策略

入站服务：用来选择允许的入站服务，可选择包括：TCP、UDP、ICMP和所有服务。服务需要在[VPN配置/高级设置/内网服务设置]里预先定义好。

出战策略

SA生存时间：用来定义第二阶段策略的生存期时间，只支持按秒计时。

出站服务：用来选择允许的出站服务。服务需要在[VPN配置/高级设置/内网服务设置]里预先定义好。

安全选项：用来选择双方协商时的安全策略，在[安全选项]标签页中进行配置。

说明：

1.如果启用了PFS，则必须保证对端VPN设备上第一阶段设置的DH组和第二阶段设置的DH组要一致，否则会导致IPSec VPN无法正常建立连接。

2. [出站策略]和[入站策略]中的[出站服务]、[入站服务]和[时间设置]均为SANGFOR扩展的规则，此类规则仅在本端设备生效，在与第三方设备建立VPN连接的过程中不会协商此类规则。

3．[出站策略]和[入站策略]中策略所对应的源IP地址是指[源IP类型]和[本/对端服务]。

安全选项

安全选项用于设置与对端建立标准的IPSec连接时所使用的安全参数。管理员可进行新增、删除、编辑安全选项操作，且所有操作都需要确定才会生效。

在建立与第三方设备的IPSec连接前，请先确定对端设备采用何种连接策略。

管理员点击<新增>安全选项需要填写名称、类型、协议类型有AH和ESP可选。

认证算法（Null或MD5或SHA-1或SHA2-256或SHA2-384或SHA2-512）

加密算法（DES、3DES、AES、SANGFOR_DES、AES192、AES256）

深信服VPN网关会使用设置好的连接策略与对端协商建立IPSec连接。

安全选项中的[加密算法]用于设置标准IPSec连接的第二阶段所使用的数据加密算法，如果要与多个采用不同连接策略的设备互联，需要分别将各个设备使用的连接策略添加到安全选项中。

说明：

1．出站策略和入站策略中策略所对应的源IP地址是指源IP类型和本/对端服务。

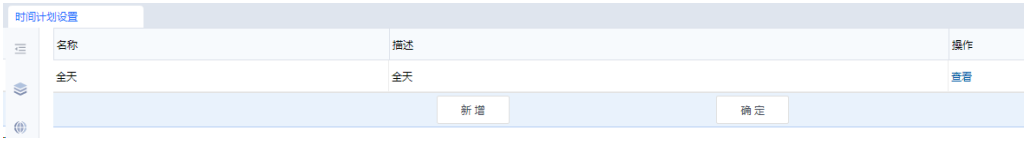
2．出站策略和入站策略中的出站服务、入站服务和时间设置均为SANGFOR扩展的规则，此类规则仅在本端设备生效，在与第三方设备建立VPN连接的过程中不会协商此类规则。

通用设置

通用设置包含时间计划设置和算法列表设置两个子模块。

时间计划设置

时间计划设置用于定义常用的时间段组合，这些时间组合可在用户管理、内网权限中使用，该时间以设备上当前时间为准。



点击<新增>按钮，出现[时间计划设置]对话框，定义了一个名称为“上班时间”的时间段，选取相应的时间段组合，然后点击<规则失效>（默认情况下，所有时间段均生效），则表示在选中时间段内规则失效，剩下则为规则生效的时间段，最后点<确定>完成时间组的定义。

说明：

管理员进行新增、删除、编辑操作，需要点击<确定>后策略才会生效。

算法列表设置

算法列表设置提供对设备支持的数据加密算法进行查看和添加的功能，加密算法会在硬件设备所构建的VPN网络中对传输的所有数据进行加密，以保障数据的安全性。

算法名称	类型	提供者	描述
DES	加密算法	Walter tuchman and Carl Meyer	Data Encryption Standard for encrypt data
3DES	加密算法	Walter tuchman and Carl Meyer	Triple-DES Standard for encrypt data
MD5	认证算法	Ronald L. Rivest of the RSA	Message-Digest Algorithm for Authentication
AES	加密算法	Joan Daemen and Vincent Rijmen	Advanced Encryption Standard for encrypt data
AES192	加密算法	Joan Daemen and Vincent Rijmen	Advanced Encryption Standard for encrypt data
AES256	加密算法	Joan Daemen and Vincent Rijmen	Advanced Encryption Standard for encrypt data
SHA1	认证算法	US National Security Agency (NSA)	Secure Hash Algorithm 1 for Authentication
SHA2-256	认证算法	US National Security Agency (NSA)	Secure Hash Algorithm 2 for Authentication
SHA2-384	认证算法	US National Security Agency (NSA)	Secure Hash Algorithm 2 for Authentication
SHA2-512	认证算法	US National Security Agency (NSA)	Secure Hash Algorithm 2 for Authentication
SANGFOR_DES	加密算法	SANGFOR VPN Group	Data Encryption Standard for encrypt data

设备内置了DES、3DES、MD5、AES、SHA-1、SINFOR_DES、AES192、AES256、SHA2-256、SHA2-384、SHA2-512多种加密、认证算法，并可以根据用户需要添加其它加密、认证算法，如需添加其它加密、认证算法请联系深信服科技的工程师。

证书管理

当客户要求使用证书方式来建立VPN，可通过证书管理中的证书请求和证书列表功能。

当设备已有有效的PKCS#12证书，可以直接在证书管理中导入，如果没有，则需要在这里申请。

证书请求

证书请求用于CER本地证书和PKCS#7证书导入，证书请求生成时会同时产生一对密钥对，用于证书导入时进行校验。

证书请求需要配置的信息包括请求名称、主题内容、拓展识别信息、密码设置，详细项配置可根据复选框的提示填写。

参数配置好点击<提交>则会生成证书申请文件和密钥文件，点击<下载>可将申请文件下载下来，下载下来的文件是一个csr的文件格式。

说明：

1. 当对应证书未导入时,删除该证书请求会影响证书的导入.建议在证书导入后在删除申请信息。
2. 证书导入最多只支持10条。
3. 系统时间在证书的生效期以外会导入失败。

证书列表

证书列表支持导入多个CA证书，包括RSA证书和商密证书。其中证书状态包括以下四种：正常：能正常使用；无效：证书校验失败；过期：系统时间不在证书生效期内；已吊销:证书被颁发证书的CA吊销。

证书列表里面导入需要用到的证书，包括本地证书和根证书导入，其他选择证书类型：选择本地证书或者根证书类型，类型有：CRE本地证书、CER根证书、PKCS#12证书、PKCS#7证书。

1. 选择CRE本地证书：

选择校验密钥：来源于申请证书列表。

CA根证书：导入申请的CA根证书。

本地证书：导入的是生成的证书。

2. 选择CRE根证书：

证书名称：根据情况自定义命名。

CA根证书：一般情况下要导入如下：

• 本地证书使用的根。

• 如果对端的证书颁发的根跟本端本地证书使用的不是同一个根，也需要导入对端的根。

3. 选择PKCS#12证书导入：

证书名称：据情况自定义命名。

CA根证书：地证书使用的CA根证书。

本地证书：入P12格式的证书。

保护密码：密码为P12格式证书生成时候的密码。

4. 选择PKCS#7证书导入:

证书名称：据情况自定义命名。

校验密钥：源于申请信息列表，即选择即将导入的证书对应的申请信息。

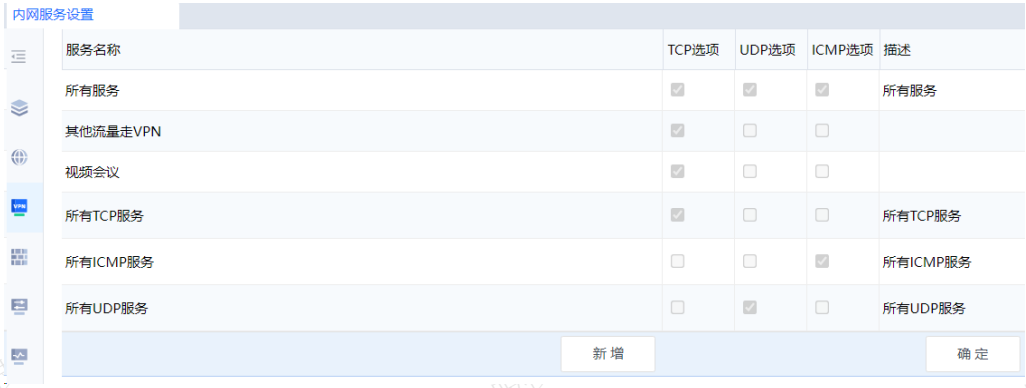
导入的根证书或者是本地证书支持下载。

高级设置

高级设置包括内网服务设置、VPN接口设置、组播服务、LDAP服务器设置和Radius服务器设置。

内网服务设置

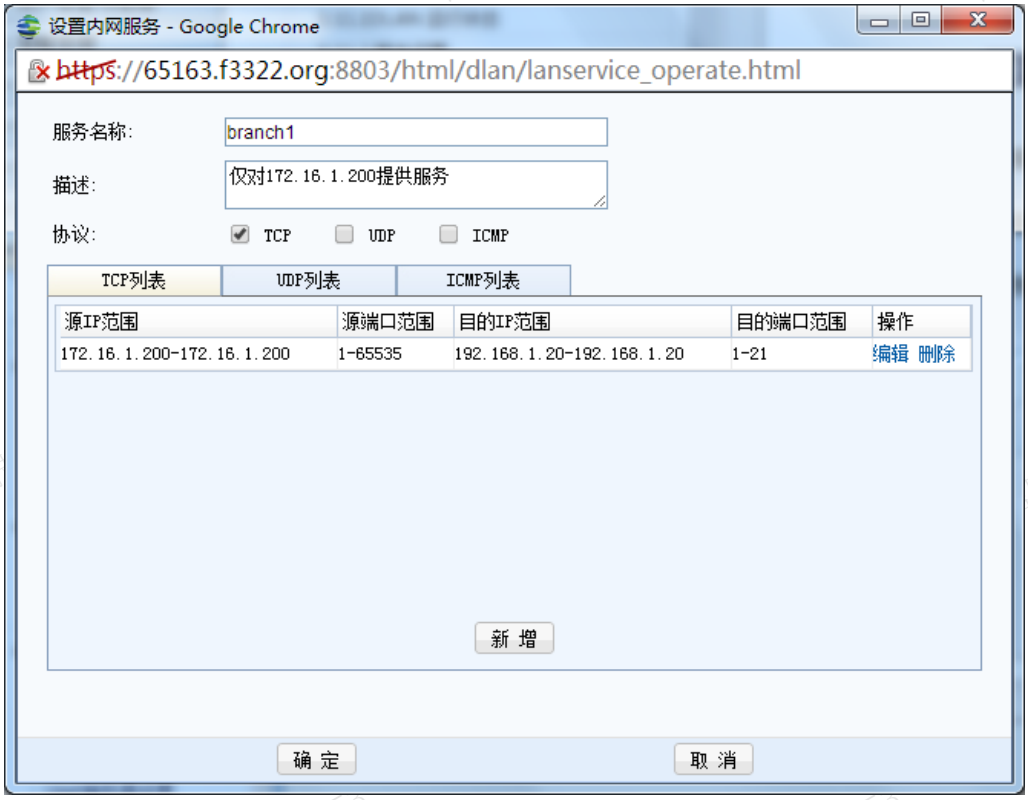
深信服设备可以为接入的VPN用户指定相应的访问权限，可以限制分支用户内网的某个IP、某个移动用户只能访问内网的特定计算机的特定服务和与第三方设备互连时设置出入站策略的服务参数。通过适当的权限设置对服务进行访问授权即可实现VPN隧道内的安全管理。



设置“内网服务权限”分为两个步骤：1、创建内网服务；2、为特定的用户指定权限。缺省状况下系统没有对VPN接入用户的访问权限做任何限制，下面例子作为说明。

当实现授权仅允许分支用户branch1的内网IP 172.16.1.200访问总部的FTP服务器192.168.1.20，其它IP发起的访问请求或对其它服务的访问请求全部拒绝，具体操作步骤如下：

步骤1.在[内网服务设置]中点击<新增>出现[设置内网服务]对话框，[服务名称]可自定义一个便于识别的名称，勾选协议类型（本例中FTP服务使用TCP协议），页面如下。



步骤2.点击<新增>出现[IP范围设置]对话框，逐项进行设置，页面如下。

源IP：本例中应设置为分支对端的内网IP 172.16.1.200。

源端口：1-65535。

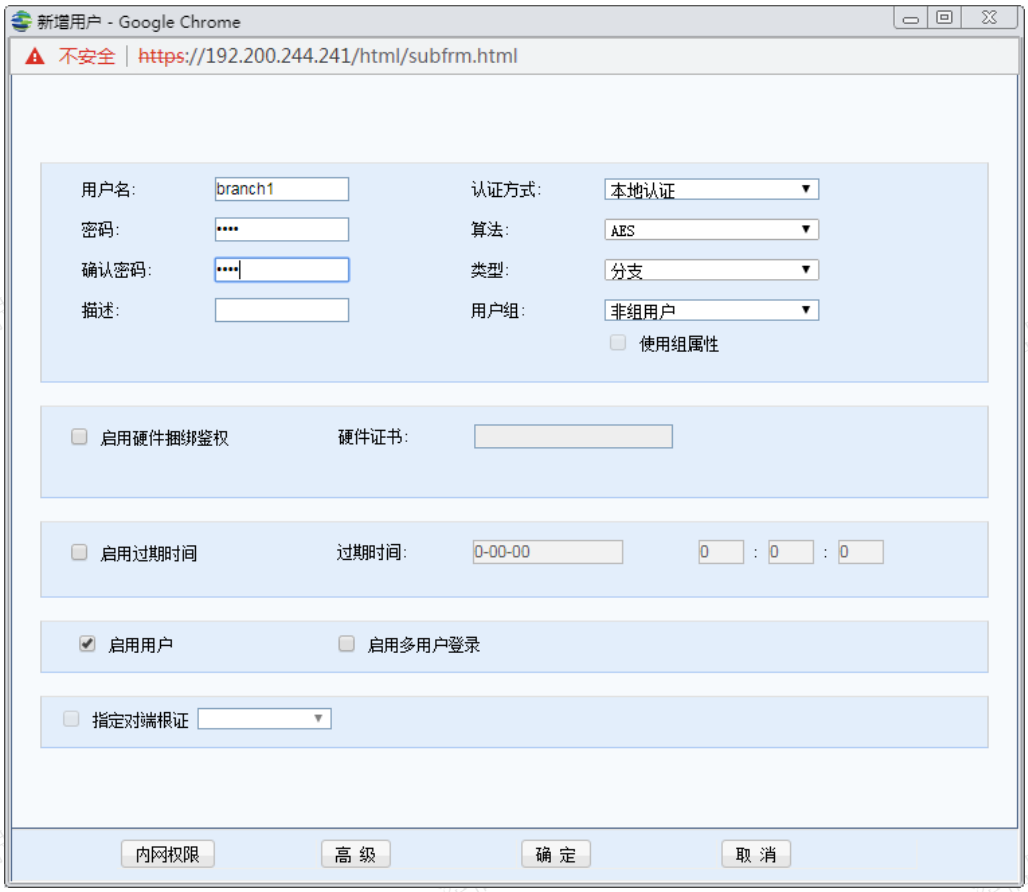
目的IP：本例中应设置为总部内网的FTP服务器IP 192.168.1.20。

目的端口：FTP的服务端口20-21。

这里的内网服务设置只是一种“定义”，定义好服务之后，需要在[用户管理]里面为用户账号分配内网权限来

最终实现“VPN内网权限”的设定。内网服务设置还可应用于[第三方对接]中设置[出站策略]的[本端服务]参数和[入站策略]的[对端服务]参数，具体设置可参考[第三方对接]相关章节。

步骤3.在[用户管理]中选择编辑用户Branch1，点击<内网权限>，页面如下。



步骤4.在内网权限对话框中将设置好的Branch1服务右移到服务列表中，设置为允许，因为本例中仅允许该服务，故将缺省动作设置为[缺省拒绝]，页面如下。

步骤5.完成以上三步设置后，即实现仅允许分支用户branch1的内网IP172.16.1.200访问总部的FTP服务器192.168.1.20，分支Branch1内网的其它IP发起的访问请求都会被拒绝。

说明

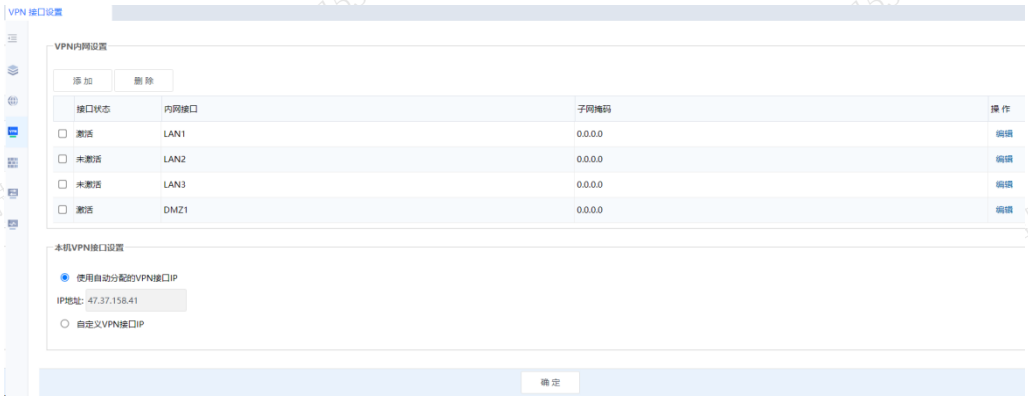
：

这样设置完成后，总部其他电脑去访问分支Branch1也一样会访问不到。因为总部其他电脑发起访问分支的

请求，分支电脑回应该请求时，因分支电脑发回的数据包里目标IP不是192.168.1.20这台服务器，也会被内网权限给拦掉。

VPN接口设置

VPN接口设置用于设置设备中IPSEC VPN服务的内网接口掩码和VPN虚拟网卡的IP及掩码，如下图。



VPN内网设置：用来设置通告VPN对端设备，本端VPN内网网段掩码。勾选了某个接口掩码，则这个接口所属掩码的网段才会被通告给VPN对端。如果DMZ口下接的网段也需要访问VPN，则也需要勾选DMZ口并且设置子网掩码。

点击<添加>，可以添加当前空闲的内网接口，设置本端VPN内网网段掩码，掩码配置0.0.0.0表示自动和网口的掩码一致。

点击<删除>，选定内网接口，删除该接口。

点击<编辑>，可以对选定内网接口的掩码进行修改。

本机VPN接口设置即设备本身VPN虚拟网卡的地址及掩码，一般情况下，使用默认地址就可以了，若出现IP冲突的提示，则可以选择[指定]并配置任意一个不冲突的IP。

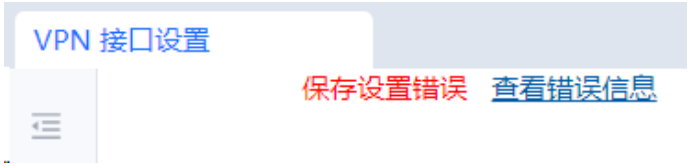
VPN接口是设备的虚拟接口，外观上并不存在对应的真实物理接口。

默认情况下请设置为[使用自动分配的VPN接口IP]，如果出现IP冲突的提示，可改为自定义IP并进行设置。

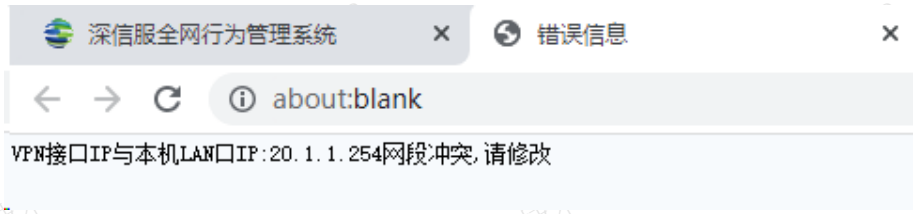
点击<确定>，提交修改。

如果配置存在错误，提交后则会报错，提示“保存配置信息出错，详情请查看错误信息”。

页面的左上角会显示保存设置错误信息后可以查看错误信息。

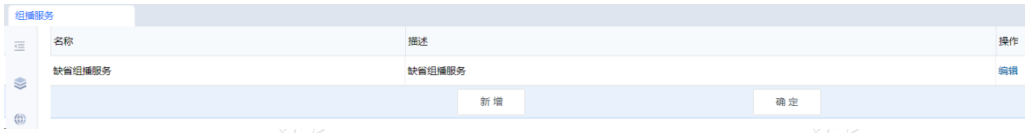


点击<查看错误信息>跳转一个新的网页，说明具体的配置错误原因。



组播服务

为满足VOIP和视频会议等应用，深信服VPN网关支持组播服务在隧道间传输。在这里可以定义组播的服务，IP范围是224.0.0.1-239.255.255.255，端口范围是0-65535。



点击<新增>出现组播服务编辑页面，在这里可以设置组播服务所用的组播地址和端口。

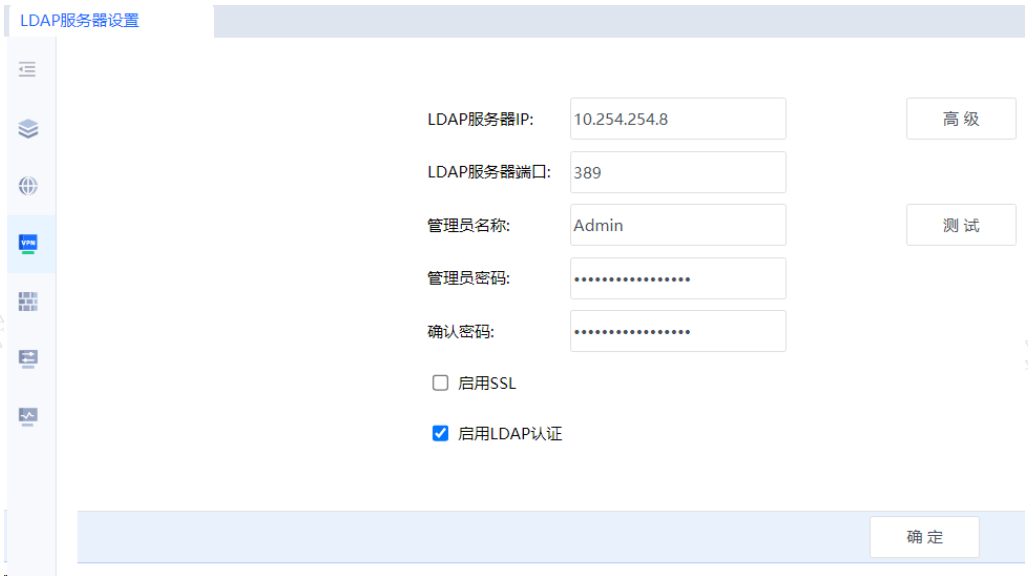
点击<新增>，添加主播的IP和端口号，如下图。

定义好以后，点击<确定>保存。

在[用户管理]新建用户时，在[组播服务]里选择刚定义好的组播服务。

LDAP服务器设置

深信服设备的VPN服务支持使用第三方LDAP认证，如需要启用第三方认证，请在[LDAP服务器设置]中正确设置第三方LDAP服务器信息（包括LDAP服务器IP、LDAP服务器端口、LDAP管理员密码），根据需求是否启用SSL和LDAP认证。



设置好LDAP服务器信息后，请点击<高级>，显示[LDAP高级设置]对话框，按照实际需求设置LDAP高级信息，如下图。

Radius服务器设置

深信服设备的VPN服务支持使用第三方Radius认证，如需要启用第三方Radius认证，请在[Radius服务器设置]中正确设置第三方Radius服务器信息（包括Radius服务器IP、Radius服务器端口、Radius认证共享密钥、Radius协议），如下图。

防火墙

防火墙包括过滤规则、NAT代理上网、端口映射、IPv6地址转换。其中NAT代理上网、端口映射、IPv6地址转换仅适用于设备做路由模式部署的情况下使用。

过滤规则

过滤规则可通过过滤规则的设置对设备各个接口之间的数据转发进行过滤，过滤的条件包括目标协议和端口、源IP、目标IP、时间等；在过滤方向中选择需要设置过滤规则的方向，包括：[LAN<->DMZ]、[DMZ<->WAN]、[WAN<->LAN]、[LAN<->LAN]、[DMZ<->DMZ]、[PN<->WAN]、[VPN<->LAN]，选择过滤方向后可以在右边页面对过滤规则进行管理、添加或删除。

需求背景

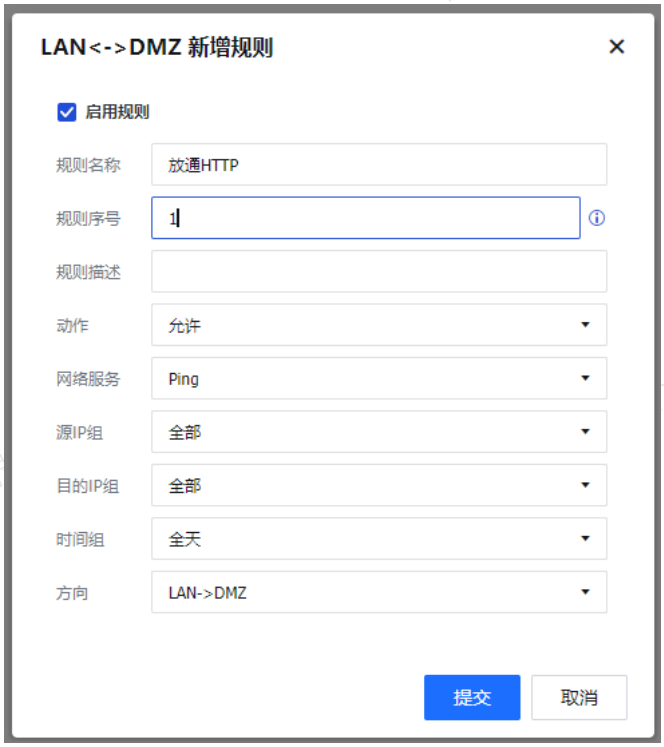
用户在设备的DMZ口区接了内网的WEB服务器，LAN口区接内网的普通用户。为保证服务器的安全，要求LAN区用户只能访问DMZ区服务器的TCP80端口即WEB服务，其他数据不允许转发到DMZ区，此时需要设置LAN<->DMZ的过滤规则。

操作步骤

步骤1.选择[过滤规则]下的[LAN<->DMZ]，右边进入[LAN<->DMZ]编辑页面，点击<新增>然后按钮，进入新增界面(如下图)。此处分别引用了对象：[对象定义/网络服务]、[对象定义/IP组]、[对象定义/时间计划组]。

步骤2.在[规则名称]中填入该规则的名称，在[规则序号]填上序号，序号是用于设置规则匹配的优先级的，序号越小优先级越高。[规则描述]用于设置此条规则的描述信息。

步骤3.设置一条规则放通LAN->DMZ的HTTP协议，选择[动作]为允许；选择[网络服务]为HTTP；[源IP组]和[目标IP组]默认选择全部，也可以指定某IP组；[时间组]选择全天，也可以指定时间段；[方向]选择LAN->DMZ。设置完成后具体如下图。



步骤4.设置完成后界面如下：用户要求只放通HTTP协议，其他数据拒绝，防火墙模块默认是拒绝的，将LAN-DMZ方向设备自带的一条允许所有的规则删除，规则中没有设置的协议数据就会拒绝，所以用户的需求设置完毕。

步骤5.如果需要编辑已经设置完成的过滤规则，点击对应的规则名称，在弹出的编辑框中即可进行编辑。

说明：

1．防火墙模块默认是拒绝的，但是lan-wan双向，lan-dmz单向这个在出厂的时候会通过配置防火墙过滤规则放通。

2．设备内置的LAN策略仅包含Lan1在有多个LAN口的情况下需要手动添加。

NAT代理上网

NAT代理上网用于设置SNAT规则，将经过设备转发的，符合条件的数据进行源IP地址转换，最常用的是设备连接路由部署NAT配置代理内网用户上网，需要设置SNAT规则进行源地址转换。在[NAT代理上网]页面可以对SNAT规则进行管理、添加和删除。配置界面如下图所示。

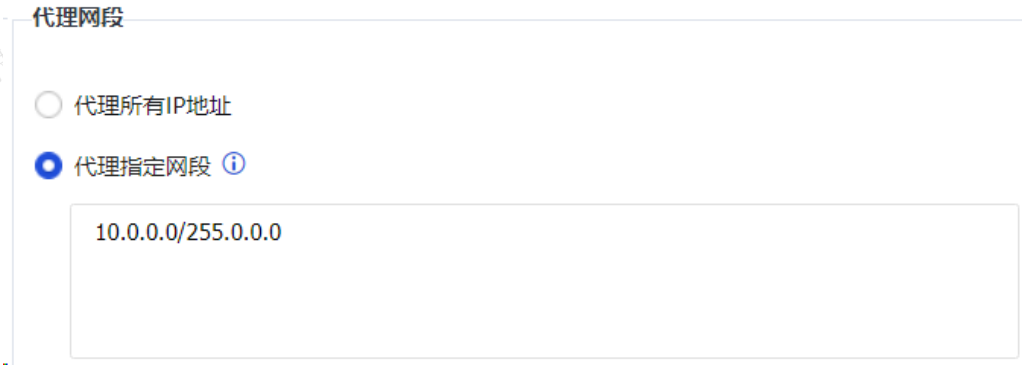
需求背景

用户内网有一个网段192.168.1.0/255.255.255.0，设备做路由模式部署，接两条公网线路，要求设备可以代理内网的用户上网。

步骤1.在[NAT代理上网]页面点击<新增>，弹出新增界面如下图：勾选[启用规则]，不勾选则规则不生效，在[规则名称]中填写规则的名称。

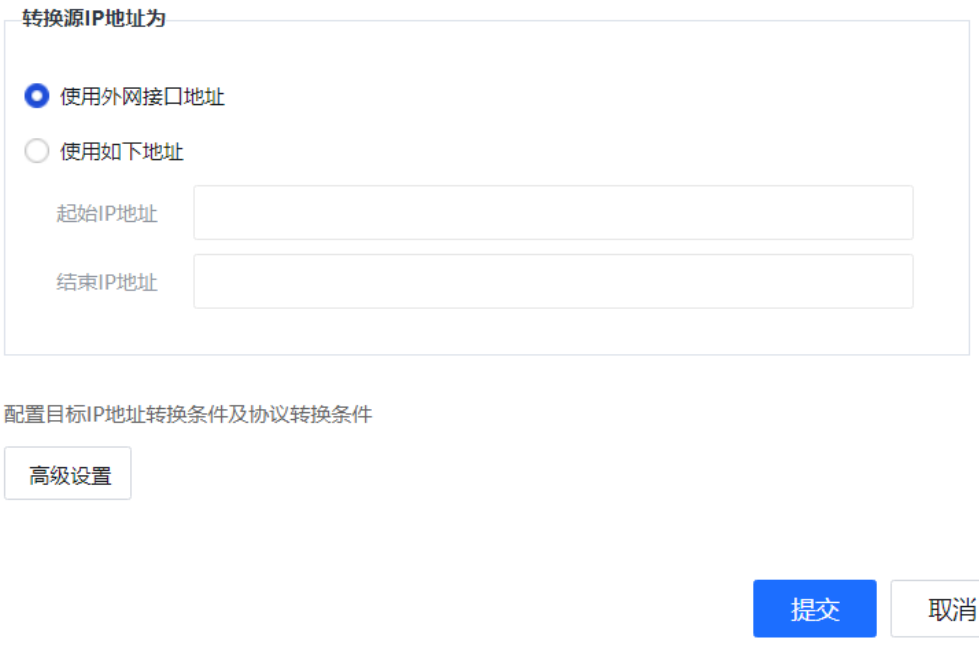
步骤2.外网接口用于设置数据转发的外网接口，是数据匹配此规则的条件之一，即数据转发的外网口。可以选择[应用于所有WAN口]和[应用于指定网口]，选择指定网口后数据只有被转发到对应的网口，才会匹配此条策略。此例中设备要代理从两个外网口转发的数据，则选择[应用于所有WAN口]。

步骤3.[代理网段]用于设置需要进行SNAT即匹配此条规则的源IP条件，可以选择[代理所有IP地址]即源IP条件不限制，也可以选择[代理指定网段]，填入指定的网段后，只有源IP条件满足才会匹配到此规则。此例中是对内网192.168.1.0/255.255.255.0网段的用户代理上网，因此指定网段192.168.1.0/255.255.255.0。



步骤4.转换源IP地址为用于设置匹配条件的数据，源地址转换成哪些IP地址。可以选择[使用外网接口地址]，勾选此项时数据的源IP会转换成步骤2中选择的外网接口的地址。也可以勾选[使用如下地址]，用于设置指定的地址进行转换。

步骤5.点击<高级设置>，用于设置更细致的匹配条件，包括目标IP地址转换条件和[协议转换条件。此例中不涉及到两种条件的设置。



如果需要编辑已经设置完成的代理上网规则，点击对应的规则名称，在弹出的编辑框中即可进行编辑。

勾选需要修改的规则，可以点击删除来删除掉该策略。

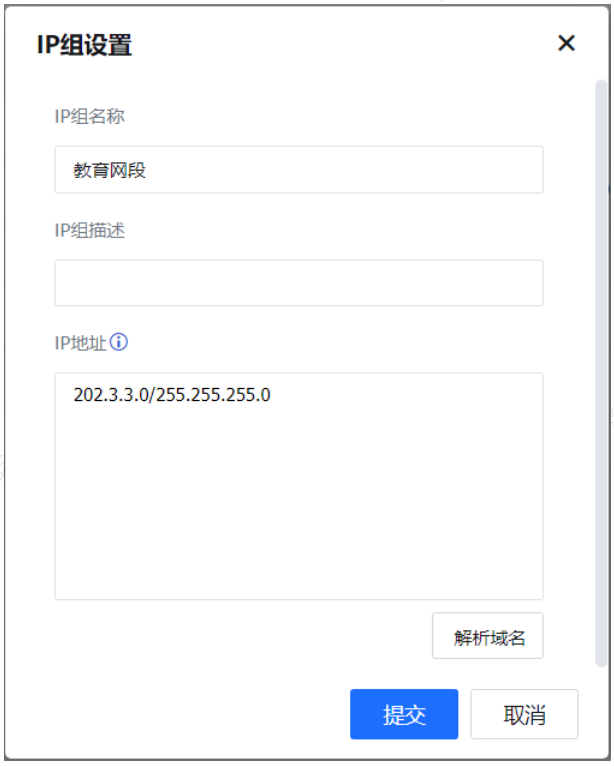
点击启用可以把规则状态改为启用。

点击禁用则把规则状态改为禁用。点击上移或者下移，则可以把规则的序号进行调整。在进行规则匹配的时候，序号靠前的规则会先被匹配到。

需求背景

设备部署成路由模式，外网有两条线路，一条电信线路，一条教育网线路，用户要求内网192.168.1.0/255.255.255.0网段的电脑在访问教育网202.3.3.0/255.255.255.0网段服务的80端口时源地址转换成教育网wan1口上的IP202.96.1.1。

步骤1.[对象定义/IP组]，分别添加IP组“教育网段”和“内网网段”，如下图“教育网段”示例填写方式，“内网网段”相同配置方式。

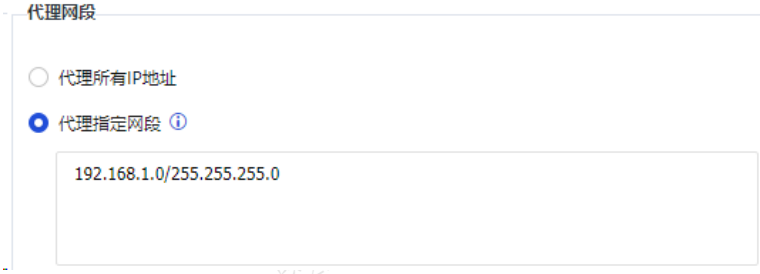


步骤2.设置[链路负载]，通过设置的链路负载自动选路，将“内网网段”访问“教育网段”的数据从WAN1即教育网线路转发。

步骤3.在[NAT代理上网]页面点击<新增>，弹出新增界面如下图：勾选[启用规则]，不勾选则规则不生效，在[规则名称]中填写规则的名称。

步骤4.[外网接口]用于设置数据转发的外网接口，是数据匹配此规则的条件之一，即数据转发的外网口。此例中是对从教育网线路WAN1口转发的数据进行地址转换，所以此处选择“WAN1”。

步骤5.[代理网段]用于设置需要进行SNAT即匹配此条规则的源IP条件，此例中代理内网网段是192.168.1.0/255.255.255.0，勾选代理指定网段设置源IP条件。



步骤6.[转换源IP地址为]用于设置匹配条件的数据，源地址转换成哪些IP地址。此例中将匹配条件的源IP转换成WAN1接口的IP202.96.1.1，所以勾选使用如下地址并设置转换的地址。

步骤7.因为此例中还有目标地址和端口需要匹配，访问教育网202.3.3.0/255.255.255.0网段服务的80端口时源地址转换，通过点击<高级设置>用于设置目标IP和转换协议的条件，如下图所示。

端口映射

端口映射用于对经过设备的数据做DNAT目标地址转换，常见应用包括发布服务器，将内网服务器的服务映射到公网，提供Internet用户进行访问，端口映射只能用于设备路由模式部署的情况下，界面如下图。

需求背景

内网一台服务器192.168.1.2，提供HTTP服务，用户要求公网用户可以访问到这台服务器的HTTP服务，设备上有两条公网线路，用户要求通过访问两条公网线路都可以访问到内网的这台服务器。

步骤1.在[端口映射]页面点击<新增>，选择新增[简单规则]或[高级规则]。

简单规则：用于简单设置一条端口映射规则，仅设置端口映射的必要条件即可。

高级规则：条件更为复杂，一般用于比较复杂的需求。

步骤2.选择[简单规则]，勾选启用DNAT规则并设置规则名称。

步骤3.[协议转换条件]用于设置匹配此条转换规则的数据条件，并且设置转换的目标地址和目标端口。

协议类型：选择需要做端口映射的数据的协议类型在；目标端口：设置组要做端口映射的数据目标端口，此例中是对访问HTTP服务的数据做NAT，则设置协议类型："TCP"，目标端口："80"。设置完条件后，设置映射到IP[映射到端口；映射到IP：用于设置数据的目标地址转换成的地址，映射到端口：用于设置数据的目标端口转换成的端口，此例中需要将访问80服务的数据目标地址转换成192.168.1.2。

步骤4.勾选[防火墙自动放行数据]用于在[过滤规则]中自动放通规则，注意勾选此项，则会放通LAN<->WAN、DMZ<->WAN、LAN<->DMZ六个方向的TCP80端口的数据。

如果需要修改已设置的端口映射规则。点击对应的规则名称，在弹出的编辑框中即可进行编辑。勾选需要修改的规则，可以点击<删除>来删除掉该策略。点击启用可以把规则状态改为启用。点击<禁用>则把规则状态改为禁用。点击<上移>或者<下移>，则可以把规则的序号进行调整。规则匹配的优先级：序号靠前的规则会先被匹配到。

需求背景

用户内网有一台服务器：192.168.1.80，设备路由模式部署，WAN1口使用光纤接入，有公网IP地址202.96.137.89，该公网IP地址对应一个域名：www.sangfor.com，现要求做一条DNAT端口映射规则把服务器发布至公网，并且要求在局域网（192.168.1.0/255.255.255.0，连接在LAN口）内的用户，也可以通过访问www.sangfor.com访问到192.168.1.80。

步骤1.在[端口映射]页面点击<新增>，选择新增[高级规则]，再弹出的[端口映射]配置界面，进行相应的配置：勾选启用DNAT规则，设置规则名称。

步骤2.外网接口是指定外网接口条件，指定从哪个接口进入设备的数据才进行DNAT。此例中域名对应的公网地址是WAN1口的地址，所以选择指定网口为“WAN1”。

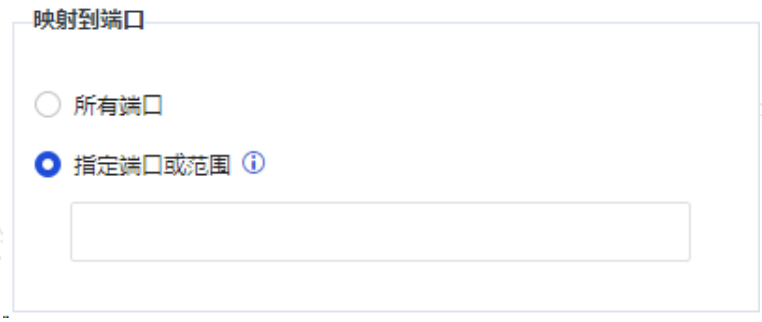
步骤3.源IP地址转换条件，用于设置DNAT转换的源地址条件，此例中因为是映射给公网，且没有指定的网段，则此处选择所有IP地址。

步骤4.设置目标IP地址转换条件，用于设置DNAT转换的目标地址条件，此例中对访问到WAN1口的IP地址的数据进行转换，则选择[指定网络接口地址]，选择“WAN1”。

步骤5.设置协议转换条件，用于设置DNAT转换的协议及端口条件，此例中是针对访问的80端口数据进行DNAT，所以此处设置如下：源端口一般是随机端口，此处选择所有端口。

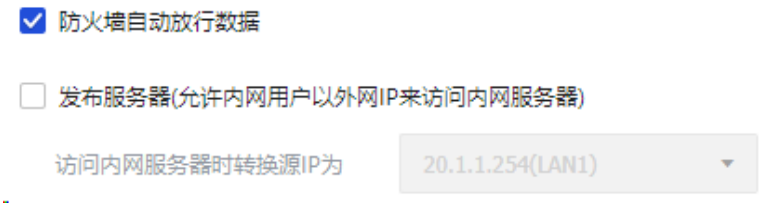
步骤6.设置映射到IP地址，用于设置匹配以上几步条件的数据，目标地址转换成哪个IP地址。此例中访问的目的服务器是192.168.1.80，则此处设置[指定IP地址]：192.168.1.80。

步骤7.设置映射到端口，用于设置匹配以上几步条件的数据。此例中是访问目的服务器192.168.1.80的80端口，则此处设置指定端口或范围：80。



步骤8.勾选防火墙自动放行数据,用于在过滤规则中自动放通规则，注意勾选此项，则会放通LAN<->WAN、DMZ<->WAN、LAN<->DMZ六个方向的TCP80端口的数据。

步骤9.发布服务器是内网用户需要通过公网IP访问到同一个网段的服务器时需要勾选，目的是将内网访问的数据源地址转换成设备相应接口的地址，避免内网用户通过公网IP访问服务器是连接无法建立成功，勾选此项设备会自动创建一条SNAT规则，进行源地址转换，此例中是LAN区的内网用户通过公网IP访问LAN区的服务器，所以此处选择[访问内网服务器时转换的源IP为]：192.168.1.12（LAN）。



IPv6地址转换

IPv6地址转换用于设置IPv6源地址转换和目标地址转换。源地址转换将经过设备转发的，符合条件的数据进行源地址转换；目的地址转换将符合条件的数据进行目的地址转换，完成IPv6前缀地址转换。

在[IPv6地址转换]页面可以对IPv6源地址转换规则进行管理、添加和删除。配置界面如下图所示。

需求背景

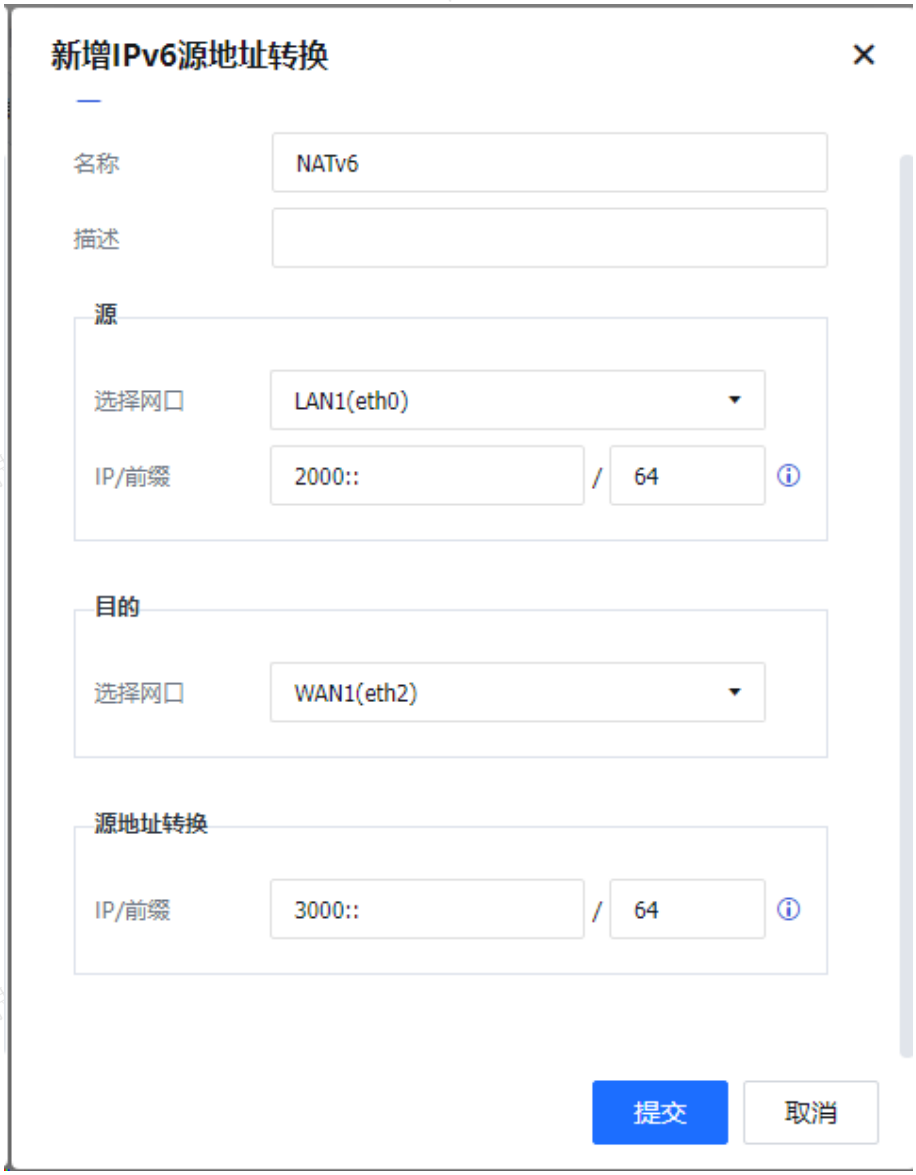
用户之前在运营商A获取了2000::/64前缀的地址，配置给了内网PC，然后由于某些原因换了运营商B，被分配了3000::/64的地址，而公司又不想花费精力去更改内部IP结构,可以使用IPV6地址转换。

步骤1.点击<新增>，选择源地址转换，填写此规则名称，描述和描述信息

步骤2.源：选择网口区域和IP/前缀，源区域选择内网网口，IP/前缀填写内网IPV6前缀地址，此例为2000::/64。

步骤3.目的：选择目的区域网口，用于设置数据转发的外网区域接口。

步骤4.源地址转换：用于设置匹配条件的数据，源地址转换成哪些IPV6地址。此案例转换为3000::/64。



步骤5.点击<新增>，选择目的地址转换，填写此规则名称和描述信息。

步骤6.源:选择网口区域和IP/前缀，源区域选择外网网口，IP/前缀填写内网IPV6前缀地址，此例为3000::/64。

步骤7.目的：选择目的IP/前缀，用于设置访问的目的地址。

步骤8.目的地址转换:用于设置匹配条件的数据，目的地址转换成哪些IPV6地址。此案例转换为2000::/64。

步骤9.添加完成配置如下图。

系统配置

系统配置包含授权管理、管理员账号、系统时间、自动升级、告警选项、全局排除地址、配置备份与恢复、终端提示页面定制、日志中心配置、高级配置、深信服设备对接，可以根据企业的需求进行详细配置。

授权管理

授权信息设置包括：设备授权、终端接入安全授权、多功能项授权、上网安全授权、应用识别&URL库升级授权、软件升级授权、上网代理授权、防泄密外发管控授权、防泄密外发审计授权和服务有效期。

不同的功能依赖于不同的授权模块，在授权管理栏内可以看到具体功能所需要的授权功能和服务的有效期。

• 设备授权：激活设备，并授权设备的线路数、分支数；查看网关序号和序列号状态是否有效；

• 终端接入安全序列号：激活终端安全检查、非法外联、外设管控、802.1x客户端认证、终端审计（U盘审计）、客户端Portal认证、客户端分时访问等模块；

• 多功能项授权：用于激活VPN配置、行为审计、内容审计、SSL内容识别等模块；

• 上网安全授权：激活僵尸网络、SAVE杀毒、恶意链接等模块；

• 应用识别&URL库升级授权：激活URL库、应用识别库和网络审计规则库、终端防泄密规则库（包括：终端应用审计规则库、终端应用文件外发管控规则库、文件类型识别特征库）、内置终端应用库等更新有效期；

• 软件升级授权：用于设备软件版本的升级；

• 上网代理授权：激活设备上网代理功能模块。

• 防泄密外发管控授权：用于激活防泄密外发管控功能（终端防泄密）模块，包含：文件外发管控策略、敏感文件识别规则。

• 防泄密外发审计授权：用于激活客户端审计策略，包含：客户端应用审计、外接设备审计、打印机审计、浏览器外发审计、解密行为审计。

授权激活方法

1. 深信服授权中心激活

步骤1.导入设备信息（该步骤在深信服授权中心完成）。

步骤2.打开浏览器，输入深信服授权中心地址：https://license.sangfor.com.cn，输入注册好的账号密码。（若没有账号密码，需注册后方可登录；云图、MSS、SAAS（云眼云盾等）账号可以直接登录）。

步骤3.初始状态下未添加任何设备，点击<现在激活>去添加设备。

步骤4.导入需要激活的设备，可以通过订单号批量添加或通过网关ID添加。（企业名称需与订单系统的名称保持一致）。

步骤5.导入设备成功，可以看到这个账号下绑定的所有深信服设备、激活状态、授权过期时间等。

步骤6.需要设备“在线激活”，必须在授权中心“启用自动激活设置”。

2. 设备激活（在设备端完成）

在线激活：

步骤1.在线激活需要配置好网络，将设备联网，输入授权ID和序列号即可激活成功。

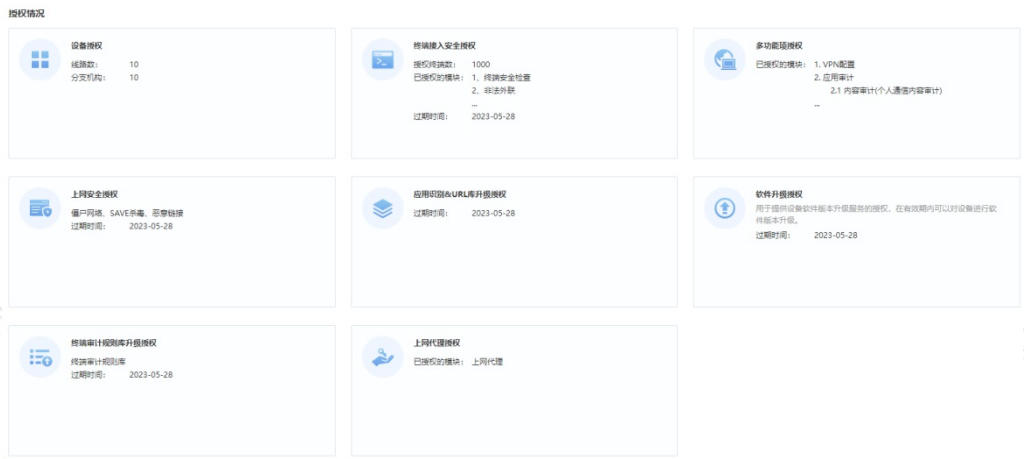
步骤2.在线激活方式还支持“主动请求激活授权”，当在授权中心完成设备信息导入后，在AC授权管理有一个<激活授权>按钮，点击主动发起请求，激活授权，输入授权ID和序列号。（授权ID和序列号请拨打销售和400-806-6868获取）。

步骤3.申请成功后会显示使用授权开启的功能、服务和具体功能参数，然后会跳转到设备登录页面。

步骤4.验证激活情况：管理员登录设备，在设备授权管理页面查看序列号状态显示：已生效，说明已经激活成功。

离线激活

步骤1.进入[授权管理]页面，点击[导出设备硬件信息]，也可以直接复制到粘贴板，用于后续生成授权文件。



步骤2.回到深信服授权中心（https://license.sangfor.com.cn），在列表中找到对应的设备，点击导出授权文件。

步骤3.将刚导出的设备硬件信息导入，点击导出授权文件，即可导出相应的授权文件。

步骤4.回到设备端，点击导入，将刚刚导出的授权文件导入到设备端，即可激活成功。

步骤5.验证激活情况：管理员登录设备，在设备授权管理页面查看序列号状态显示：已生效，说明已经激活成功。

管理员账号

管理员账号用来设置能够通过控制台来管理设备的登录用户和管理员角色管理。设备出厂默认的管理员的账号密码为：admin/admin。在导航菜单页面中的[系统管理/统配置/管理员账户]，进入管理员账户编辑页面，进行新增、编辑、删除、启用和禁用操作。

本地管理员账号

步骤1.创建管理员账户。在[系统管理/系统配置/管理员账号]，点新增后，跳转到管理员账户的编辑窗口，填写管理员账户的用户名和描述信息。管理员角色即为该用户选择第一步描述的管理员角色，设备内置四个角色：administrator、系统管理员、安全管理员、审计管理员。

步骤2.登录安全设置中的设置登录控制台的密码。

步骤3.Dkey是日志中心查询功能时必须使用Dkey。点击<生成Dkey>设置DKAY的登录密码。

步骤4.限制登录配置用于限制管理员登录控制台的IP地址。可以设置单个IP也可以设置IP段，一行一条设置最多可以设置32行。

步骤5.对创建的账户设置[组织权限设置]，用于设置控制台用户管理用户组的权限，用户组可以选择，点击<选择>，列出设备中的组织结构，选择可以管理的组即可。

步骤6.超级管理员administrator角色不能配置“组织权限设置”的，默认是所有权限。

步骤7.设置页面权限，定义管理员是否有各个模块可查看或者是可编辑的权限。

超级管理员administrator角色是不能配置“页面权限设置”的，默认是所有权限；

内置的系统管理员、安全管理员、审计管理员角色也各自有默认的页面权限，可以依据实际需求进行增删权限。

步骤8.完成配置后，点击<提交>，完成了新增一个本地密码管理员账号的配置。

账号密码认证+USB-key认证

管理员账号增加双因素认证，默认功能不开启。想要使用在对应管理员账号[认证策略]进行选择，用到USB-key。

步骤1.准备AC设备一台，红色USB-Key一个。

步骤2.管理员日常使用Windows7/8/10/服务器电脑一台。

步骤3.win7电脑打开IE浏览器（win8以上电脑以管理员身份运行打开IE浏览器）。

步骤4.使用超级管理员admin或系统管理员登录设备控制台。

步骤5.进入[系统管理/系统配置/管理员账号]认证策略选择“账号密码认证+USB-key认证”。

步骤6.绑定U-key点击“去生成UEB-Key”。

步骤7.如果使用不是Windows电脑或IE浏览器会报错。

步骤8.根据提示“生成USB-Key前需要先配置内置根证书，是否现在前往进行配置”，点击<关闭>。

步骤9.这里配置的是“谁颁发（根证书）给（管理员账号）”，未配置过的新设备才会提示。

步骤10.点击<立即配置>，完成信息填写，点击<提交>。

步骤11.检查下前面的配置，点击<证书管理>查看内置根证书的配置或进行修改。

步骤12.也可以在[设置/证书管理]，查看整改管理的信息和修改配置。

步骤13.点击查看，可查看证书的详细内容。

步骤14. 点击<修改配置>，可以根据需求进行修改。

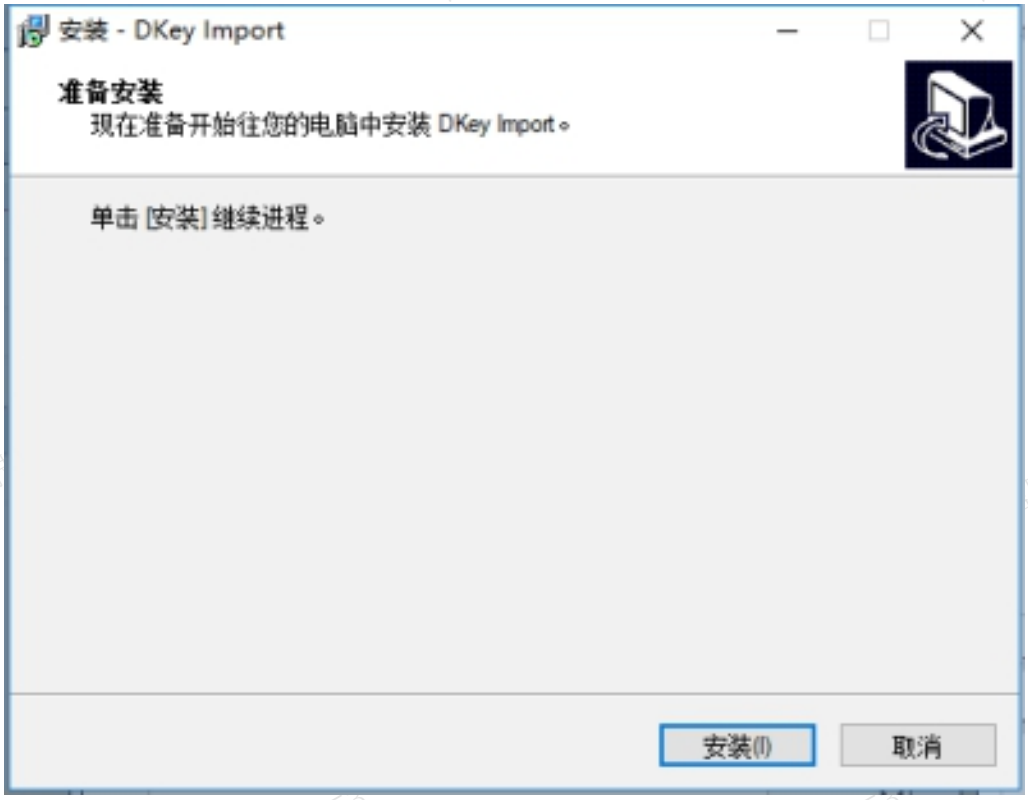
步骤15.服务重启后，回到[管理员账号]配置页面，继续生成USB-Key。

步骤16.电脑插入key。

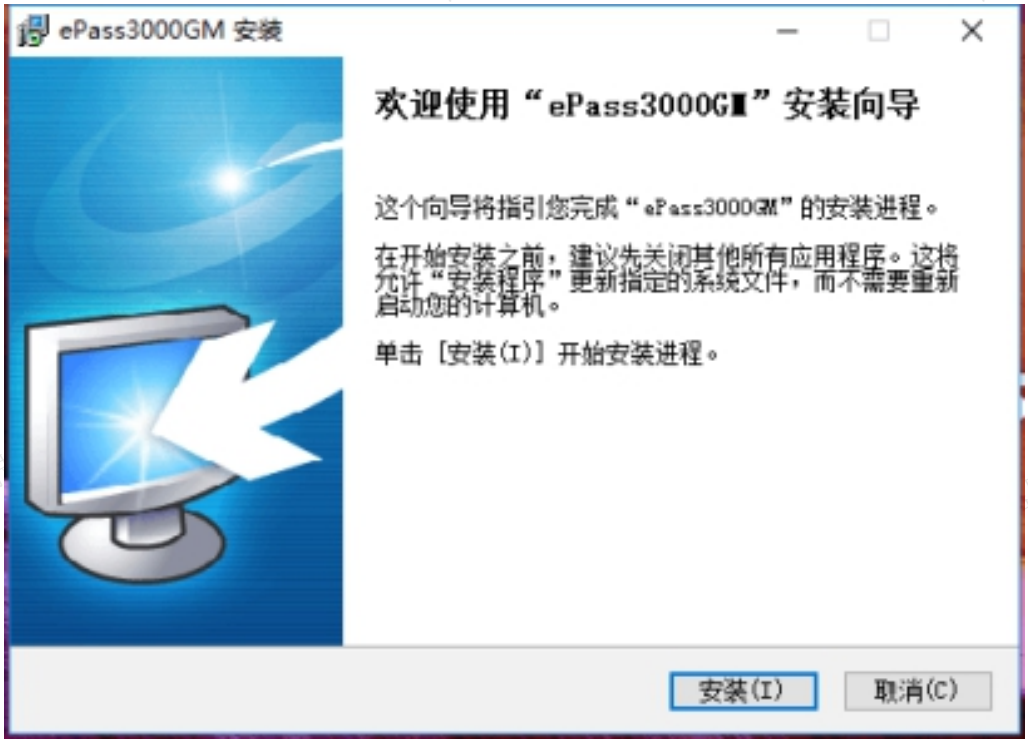
步骤17.回到管理员账号配置页面，继续生成USB-Key。“提示：当前版本暂时不兼容，无法使用此功能”

步骤18.可以勾选“记住该次配置，以后默认使用”，没有下载过驱动的，可在这个页面下载驱动（两个安装文件）。

步骤19.Dkey Import3.0.exe的安装教程。



步骤20.ePass3000GM.exe安装教程。



步骤21.分别运行安装，完成后返回控制台（熟练的情况可以先完成驱动的安装）。

步骤22.安装完成后，点击<重新检测>。

步骤23.自定义输入PIN码后，提交烧录key。完成烧录成功，可以看懂绑定U-key。

步骤24.管理员账号列表看到认证策略变成“账号密码认证+USB-Key认证”。

步骤25.登录账号在控制台页面，输入双因子认证的账号。 提示：需要插入USB-Key登录。插入key以后，弹出PIN码框。完成登录，直接拔掉key：有弹框提示，并会注销AC控制台登录。

账号密码认证+邮件验证

管理员账号增加双因素认证，默认功能不开启。想要使用在对应管理员账号[认证策略]进行选择（注意：admin账号不建议启用该功能）。

步骤1.管理员账户中新增管理员账户，填写用户名和描述。

步骤2.在登录安全设置中[认证策略]选择“账号密码认证+邮件验证”，填写接收验证码的邮箱地址。

步骤3.配置邮件告警：[系统管理/系统配置/高级配置/通知设置]，邮件通知服务器需要保障是可以成功发送邮件的，否则将影响控制台的登录。

步骤4.完成配置后，登录设备控制台，没有配置[邮件验证]的账号，正常登录控制台。

步骤5.有配置[邮件验证]的账号，出现验证码框。

步骤6.输入邮箱收到验证码。

步骤7.完成认证，登录控制台。

角色管理

角色管理是用来创建管理员角色。设备默认提供四个内置角色：administrator、系统管理员、安全管理员、审计管理员。内置的角色都具备默认的[组织权限设置]和[页面权限设置]，administrator超级管理员是所有权限。

管理员角色列表中，其排列顺序决定了权限级别的高低顺序。在管辖范围相同的情况下高角色级别的管理员可以修改低角色级别管理员创建的策略，并且自己创建的策略优先于低级别管理员的策略。定义角色时，除

超级管理员权限外，都需要定义[组织权限设置]和[页面权限设置]。

说明：

1. 不同角色优先级别不一样，从上到下，越往下新增角色优先级越低。
2. 低优先级角色的管理员不能对优高优先级的管理员的对象进行删除和修改操作。

三权分立

设备提供三种系统管理员、安全管理员、审计管理员三个内置的管理员角色。每个管理员负责不同的职责，实现三权分立。

系统管理员：负责对软件环境日常运行的管理和维护，以及对系统的备份和操作系统恢复（部署、网络配置、备份等等）。

审计管理员：拥有对系统日志、管理员操作日志进行查看、导出的权限。

安全管理员：负责业务配置、应用管理、授权管理等操作（业务配置、策略配置等）。

注意事项&排错

1. 如果在生成USB-KEY过程中出现问题，一般按照系统提示都能解决问题，请检查以下几点：

• 生成USB-KEY仅支持IE浏览器，win8以上电脑需要使用管理员权限运行IE浏览器，请检查是否使用管理员权限打开了IE浏览器。

• 生成USB-KEY需要浏览器控件支持，请在 USB-KEY信息操作界面检测是否已安装控件，安装控件后，需要重启浏览器生效。

2. 生成USB-KEY需要USB-KEY驱动支持，请检查是否已经安装并启动了USB-KEY驱动，即插拔USB-KEY系统托盘是否会有提示。USB-KEY驱动程序名为：USBKey管理工具（certreg MFC Application）。
3. 操作USB-KEY时，PC只能插入一个USB-KEY，如果有插入多个KEY请拔出21q98oiukjmn 多余的KEY。如果是使用需要USB-KEY认证登录的管理员在操作USB-KEY生成，在生成USB-KEY操作时，是允许临时拔出当前管理员的KEY的，只保留需要烧写的USB-KEY即可。
4. USB-KEY认证用户登录失败。

USB-KEY登录功能对PC系统和浏览器的兼容性有要求，请先检查当前的系统和浏览器是否支持。以下是已经保证支持的主流场景，其他场景不能保证。

3	组件	操作系统兼容性	浏览器兼容性	应用软件的兼容性	其它方面的兼容性
14	DKEY(烧key、登录)	烧key： win7、win8、win10、windows server2012 Dkey登录： win7、win8、win10、windows server2012	烧key： IE8、IE9、IE10、IE11 Dkey登录： IE9、IE10、IE11、chrome	不涉及	不涉及

5. 如果出现UKEY认证失败：

• 请检查USB-KEY是否正确且已经插入。

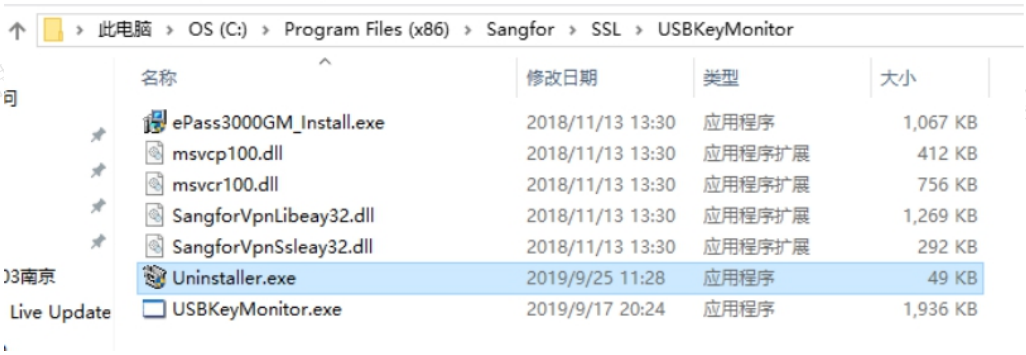
• 请检查USB-KEY的证书是否已经过期，设备时间和PC时间是否差距过大。

• 如果刚使用浏览器登录了其他USB-KEY用户，或者该USB-KEY是刚生成后立即使用的，请尝试清除浏览器SSL缓存或直接重启浏览器后再重新登录。

6. USB-KEY登录仅支持一个Key，请不要在PC上插入多余的USB-KEY。

7. USB-KEY驱动卸载。

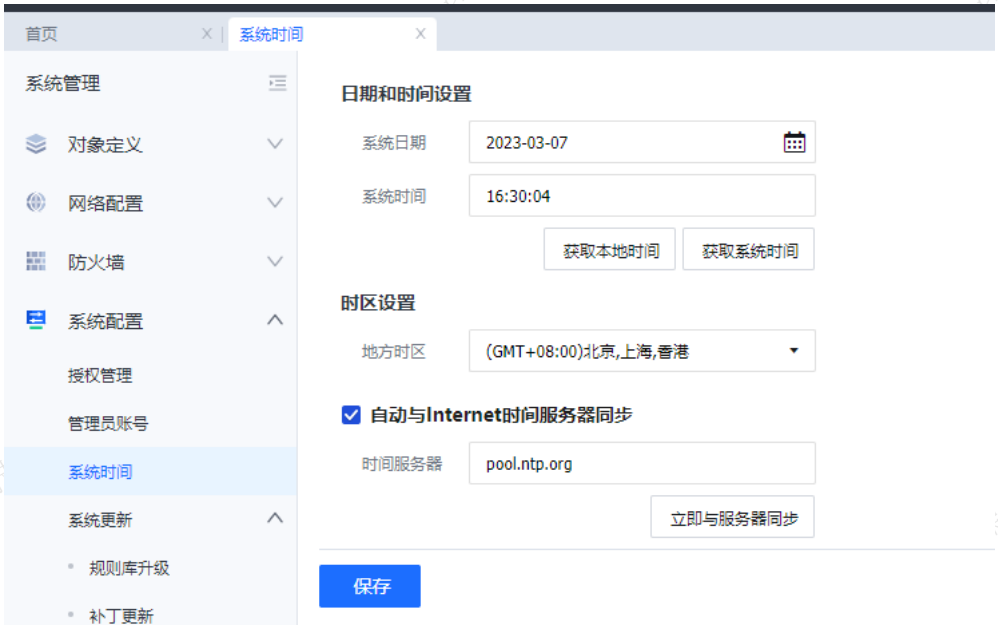
安装了驱动的电脑，进入到C:/Program Files (x86)/Sangfor/SSL/USBKeyMonitor路径，双击执行Uninstaller.exe 可以同时卸载两个驱动。卸载需要重启电脑。



如果在控制面板-应用-卸载应用进行卸载会出现卸载不干净的问题，可以手动到安装路径（C:/Program Files (x86)/Sangfor/SSL/USBKeyMonitor路径）清理没卸载干净的文件。

系统时间

系统时间用于设定深信服设备的系统时间。可以直接在界面上修改时间，也可以选择与[时间服务器]进行时间的同步。



日期和时间设置：用于查看系统的当前时间，也可以在此处手动设置系统时间。

点击<获取本地时间>，则设备的系统时间会和登录控制台的电脑时间一致。

点击<获取系统时间>，可实时刷新设备系统本身的时间。

设备的系统时间也可以设置成和时间服务器同步，在时区设置中选择设备所在的时区，勾选[自动与Internet时间服务器同步]，设置公网的时间服务器，设备会自动与此时间服务器的时间进行同步。

说明：

当管理修改时间，设备会重启服务和断网，请在业务空闲的情况下操作。

系统更新

系统更新用于对系统升级、代理设置、自动升级、补丁包更新功能进行配置和管理。

系统升级

系统升级用于设备系统版本升级，详细操作请参考产品升级指导章节。

代理设置

在本机设备无法联网的情况下，通过配置代理服服务器升级内置库。

1. 启用代理服务器；
2. 配置代理服务器的IP和端口；
3. 勾选验证用户，并输入代理服务器需要验证的用户名和密码；
4. 点击<保存>配置完成。

规则库升级

规则库升级用于对设备的SAVE引擎库、URL库、应用识别库、网络审计规则库、终端防泄密规则库、内置终端应用库进行升级管理。管理员可通过点击启用、禁用内置库的自动升级，确保设备可以上网。

1. 通过点击“立即更新”即可完成在升级服务有效期内的规则库的手动升级。
2. 点击“回滚”可以将相应的规则库回滚到最近一次升级前的规则库。
3. 点击<升级服务器配置>进入[升级服务器配置]页面。

说明：

1. 服务器设置：用于配置设备需要连接的升级服务器，一共有上海服务器、深圳服务器、备用服务器、自动选择服务器。
2. 建议选择[自动选择服务器]，让设备自动检测可以连接的更新服务器。

补丁更新

深信服OLU内网补丁服务器也可以通过手动导入更新补丁包功能，实现设备离线自动安装补丁，有效解决内网有大批量设备补丁更新的问题。

有如下几种方式：

1. 设备能与在线补丁服务器连通时自动获取补丁；
2. 设备通过代理服务器访问外网时，配置代理服务器获取补丁包；
3. 设备无法访问外网时，通深信服OLU内网补丁服务器获取补丁包；
4. 设备不能与在线补丁服务器连通，但是访问设备控制平台的PC可以上网时：通过PC浏览器访问深信服在线补丁服务器获取补丁；
5. 设备不能与在线服务器连通，且本机PC无法上网时：可使用手机扫描二维码方式获取离线补丁。

详细配置请参考补丁更新指导章节。

告警选项

告警选项的事件包括：告警事件、邮件告警、Syslog告警、SNMP Trap告警。

当设备检测到有攻击、发现移动终端、发现病毒、磁盘剩余空间不足、流量超限、日志中心异常、CPU和内存占用过高、序列号过期、关键业务检测、网络故障等事件时，以邮件、Syslog或Snmp trap的方式通知管理员进行告警。

告警事件

在[系统管理/系统配置/告警选项/告警事件]，勾选[启用事件告警]用于开启设备的事件告警功能。管理员可根据需求勾选安全事件告警和平台状态告警。告警邮件设置默认使用全局配置。如需设置不同的收件箱及发送频率，请分别设置。

点击<流量超限告警设置>，用于设置流量超限告警。可设置包括上行流量、下行流量和总流量的持续时间及流量阈值。例如：分别设置5、100，表示流量超过5分钟超过100Kbps时会告警，不勾选相关选项或者将[持续时间]和[流量阈值]设置为0，都表示不告警。点击<确定>生效。

点击<CPU占用过高告警设置>，用于设置CPU过高告警。可设置持续时间、占用阈值。例如：分别设置5和90，表示CPU占用超过5分钟超过90%时会告警，不勾选相关选项或者将[持续时间]和[占用阈值]设置为0，都表示不告警。

点击<内存占用过高告警设置>，用于设置内存占用过高告警。可设置持续时间、占用阈值。例如：分别设置5、90，表示内存使用率超过5分钟超过90%时会告警，不勾选相关选项或者将[持续时间]和[占用阈值]设置为0，都表示不告警。点击<提交>生效。

点击<关键业务检查告警>，用于设置关键业务检查告警，采用定期ping包的方式，检测业务是否正常。可设置检查频率、检测发包数、量、待检测的目标主机。

检测频率（分钟）：对待检测目标地址每轮检测之间的间隔时间。

检测发包数量：对于一个目标地址在一轮检测中的发包数量，如果在一轮检测中发送的ping包100%丢失，则认为该主机无法正常访问。

待检测的目标主机：设置需要检测的目标主机，一行一个IP地址或域名（支持IPv4、IPv6、域名），不支持IP段和子网，最多可设置64个目标主机。

邮件告警

邮件告警一般是在设备出现拒绝服务或是服务器状态时通过设置邮件告警来通知管理员或者其他用户。

配置思路：

1. 管理员需要先配置告警事件，可根据需求可选安全事件告警、平台状态告警、其中邮件告警需要配置发送设置。
2. 配置告警接收方式，其中邮件告警还需要配置发送邮件通知的服务器。
3. 配置邮件服务。

告警邮件发送设置：邮件发送默认使用全局配置。

如需设置不同的收件箱及发送频率，请点击<告警邮件发送设置>，根据告警事件进行自定义发送编辑设置。

邮件告警可设置收件地址、邮件标题、最短发送间隔。

- 收件箱：设置有告警邮件需要发送时，接收的邮箱地址。
- 邮件标题：用于定义通知邮件的标题。
- 最短发送间隔：用于设置告警邮件发送的时间间隔。
- 点击<配置发送邮件服务器>会跳转到邮件服务器发送页面，请参考通知设置邮件服务器章节。

Syslog告警

在[系统管理/系统配置/告警选项/Syslog告警]中的Syslog告警是将系统日志发送到外部Syslog服务器上。

需要设置相关服务器时，需要点击<Syslog告警设置>跳转到[系统设置/高级选项/配置外部syslog服务器]。

Snmp trap告警

在[系统管理/系统配置/告警选项/Snmp trap告警]中的Snmp trap告警是将告警发送到外部的客户端上。

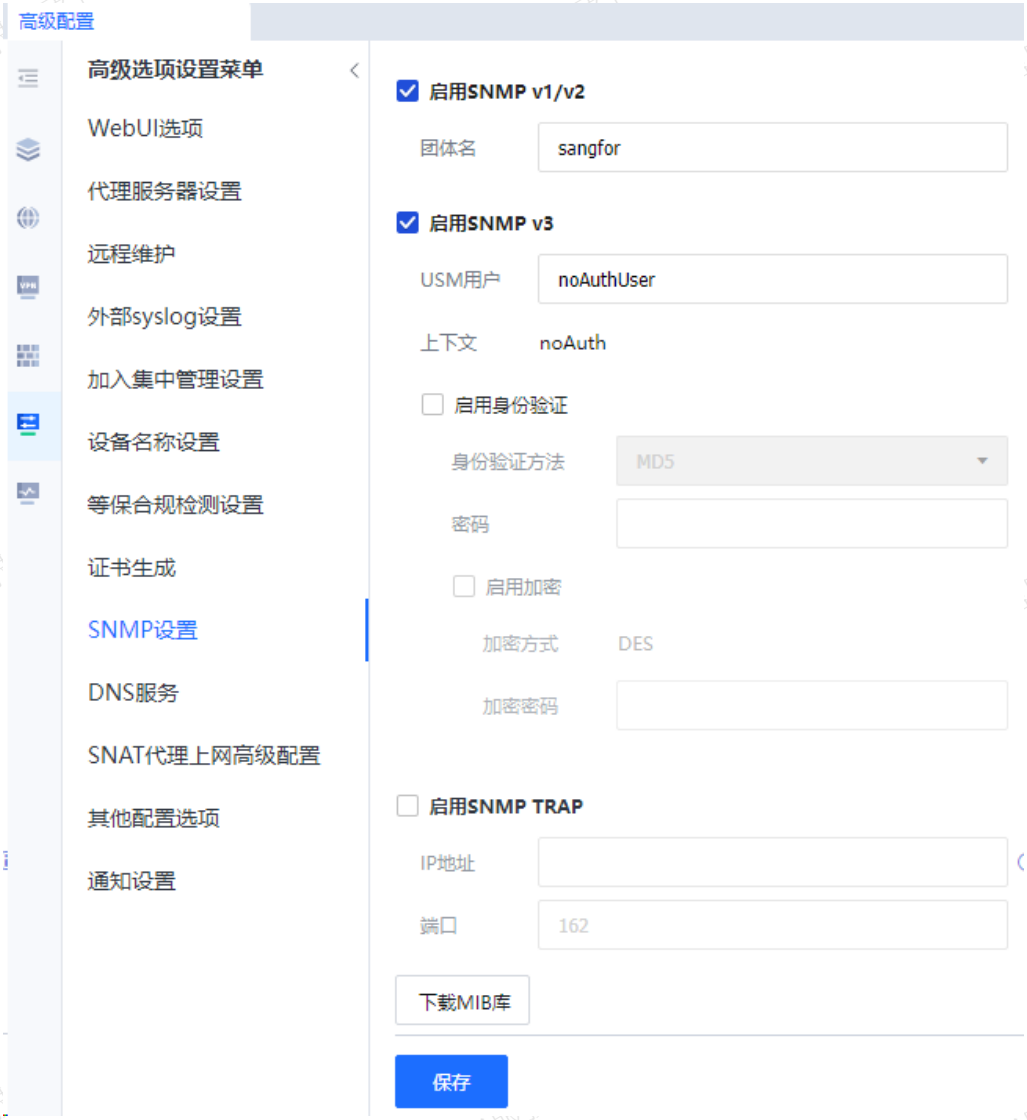
点击<Snmp trap告警设置>跳转到[系统设置/高级选项]，启用Snmp及Snmp trap功能对接Snmp服务器。Snmp trap对接配置参考SNMP章节。

SNMP TRAP配置案例

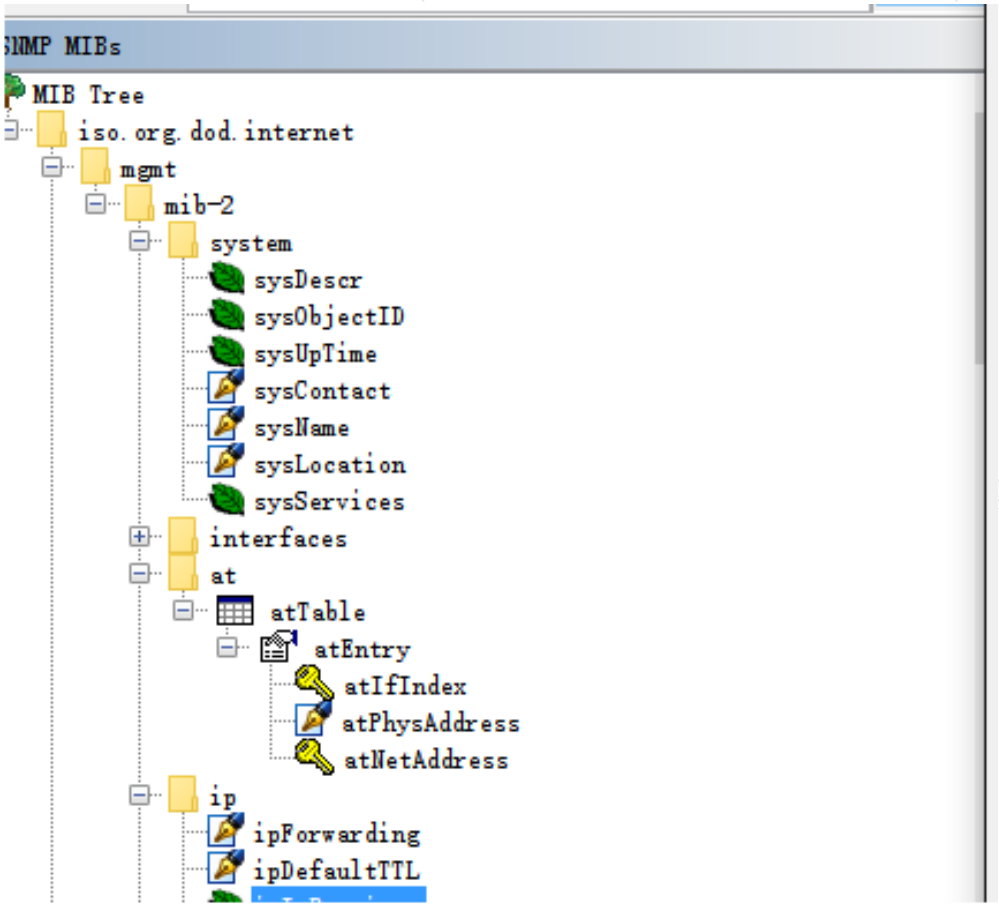
步骤1.配置[告警选项/告警事件]，测试中为了效果方便显示，把内存占用过高告警设置，定义为如图最小值。

步骤2.配置Snmp trap告警。

步骤3.启用SNMP，启用Snmp trap，配置trap服务器IP和端口。

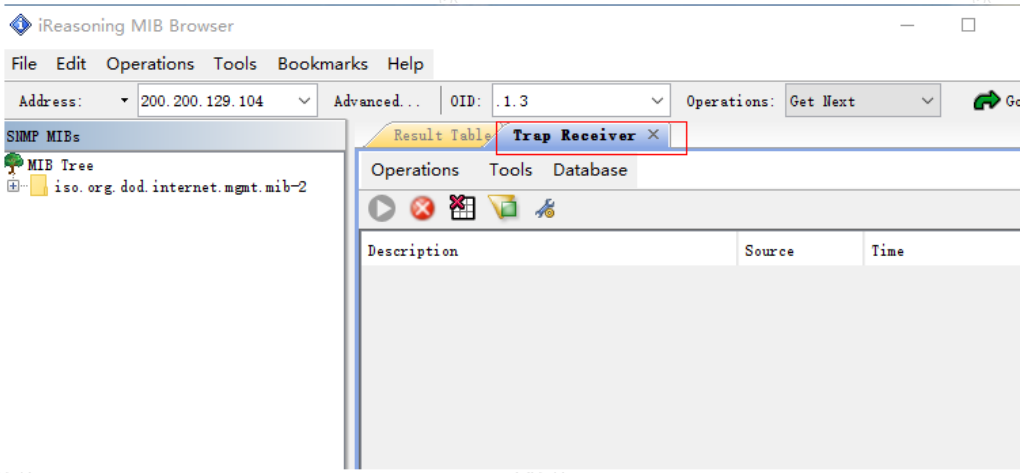


步骤4.SNMP Trap配置，文档使用mib browser工具测试，导入SG的mib库。

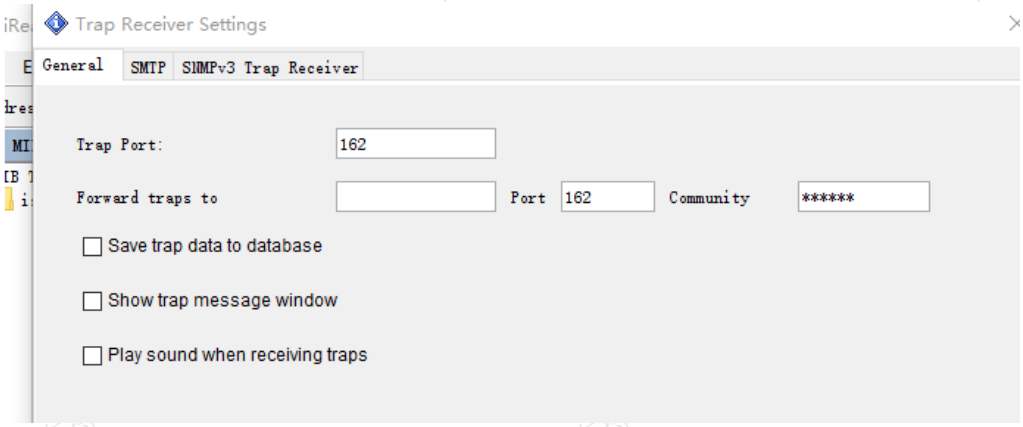


步骤5.本文中配置的是SNMPV1V2，服务端配置的SNMPV2。

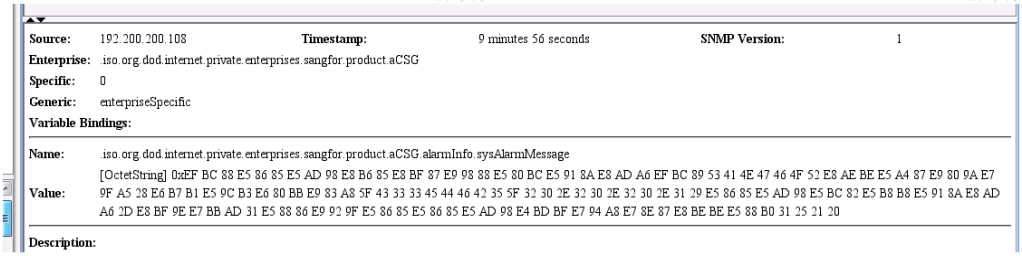
步骤6.点击Tools-Trap Receiver。



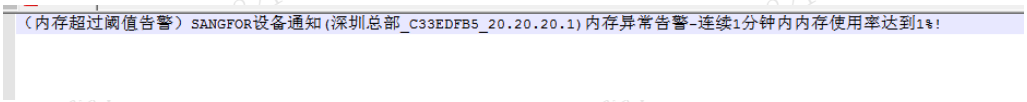
步骤7.Tools-General这一页配置项确认端口和团体名与AC一致。



步骤8.完成配置后，等待告警主动发送，测试环境没有做转码，所以出现的是16进制的值。



步骤9.人工转码后。



全局排除地址

全局排除地址就是排除IP地址，可在NAT、端口映射、显示代理、防DoS攻击 、ARP欺骗防护、系统路由和链路负载等功能引用。

当内网用户IP或访问的目标服务器的IP属于[全局排除地址]列表中的IP时，内网用户上网或访问目标服务器，不受任何监控和控制，直接放行。排除地址支持填写IPV4地址、IPV6地址、域名。

内置排除地址：是设备内置的一些地址，包括各种杀毒软件更新升级连接的服务器，避免更新升级时因为和用户策略冲突导致无法更新的问题。内置排除地址可以禁用但不能删除。

自定义排除地址：提供给用户自己添加需要排除的地址，点击<添加>，跳转到新增自定义排除地址页面，填上描述信息和需要排除的地址。

说明
：

1．全局排除地址在防火墙中不生效。

2．当AC的DNS不一致可能解析出来的IP会不一致，导致PC访问的真实IP和AC排除IP的不一致而出现不生效的情况。

配置备份与恢复

配置备份与恢复用于将设备已有的配置下载保存，或者是将已备份的配置文件恢复到设备中。

默认设备每天凌晨自动备份配置文件在设备本地，系统会保留最新的30天备份记录。超过30天的备份配置文件将会被删除。

备份配置：用于备份下载设备中已有的配置，点击<下载当前的配置>，就可以对当前的配置进行备份。

恢复配置：用于恢复已备份的配置文件，有两种方式。

方式一：从自动备份中恢复，设备会在每日凌晨自动备份一次配置，默认保存一个月的配置文件，选择会要恢复的配置文件。

方式二：从本地文件中恢复，点击浏览本地文件，并打开备份文件，点击恢复即可恢复备份配置。

说明
：

1．恢复备份（不恢复网络配置）不会重启设备。

2．恢复备份（含恢复网络配置）会重启设备。

恢复出厂设置：用于将设备恢复到出厂设置，不包括数据中心的日志，请慎用。

设备每天凌晨自动备份的配置文件也支持通过邮件或FTP备份到外置服务器。

备份到邮箱：用于将设备自动备份的配置文件通过邮件备份到外置服务器，需要在设备提前配置邮件服务器，可参考11.5.11.13通知设置章节。（一封邮件最大发送20M附件，当设备的配置文件超过20M时，会自动通过拆分的方式发送多封邮件）

收件地址：接收备份文件的邮件地址。

邮件标题：可以自定义邮件标题，也可以置空。

备份到FTP服务器：用于将设备自动备份的配置文件通过FTP备份到外置服务器。

FTP服务器地址：填写用于存储备份文件的外置FTP服务器IP地址。

服务器端口：填写FTP服务器端口，默认TCP21。

导出路径：填写FTP服务器备份文件存储路径，存储路径不支持填写中文路径。

FTP身份认证：填写登录FTP服务器的用户名/密码，如FTP服务器不需要认证，可不勾选。

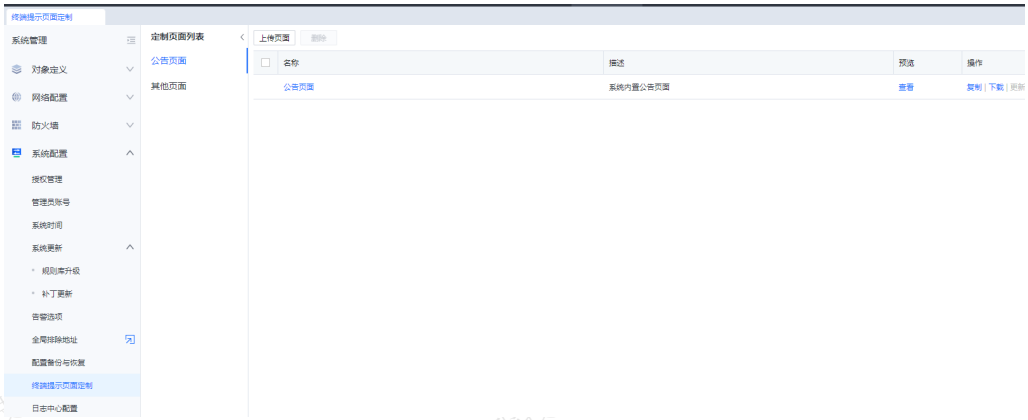
终端提示页面定制

终端提示页面定制用于对设备重定向到终端的页面进行自定义，可以定义的页面分公告页面和其他页面。

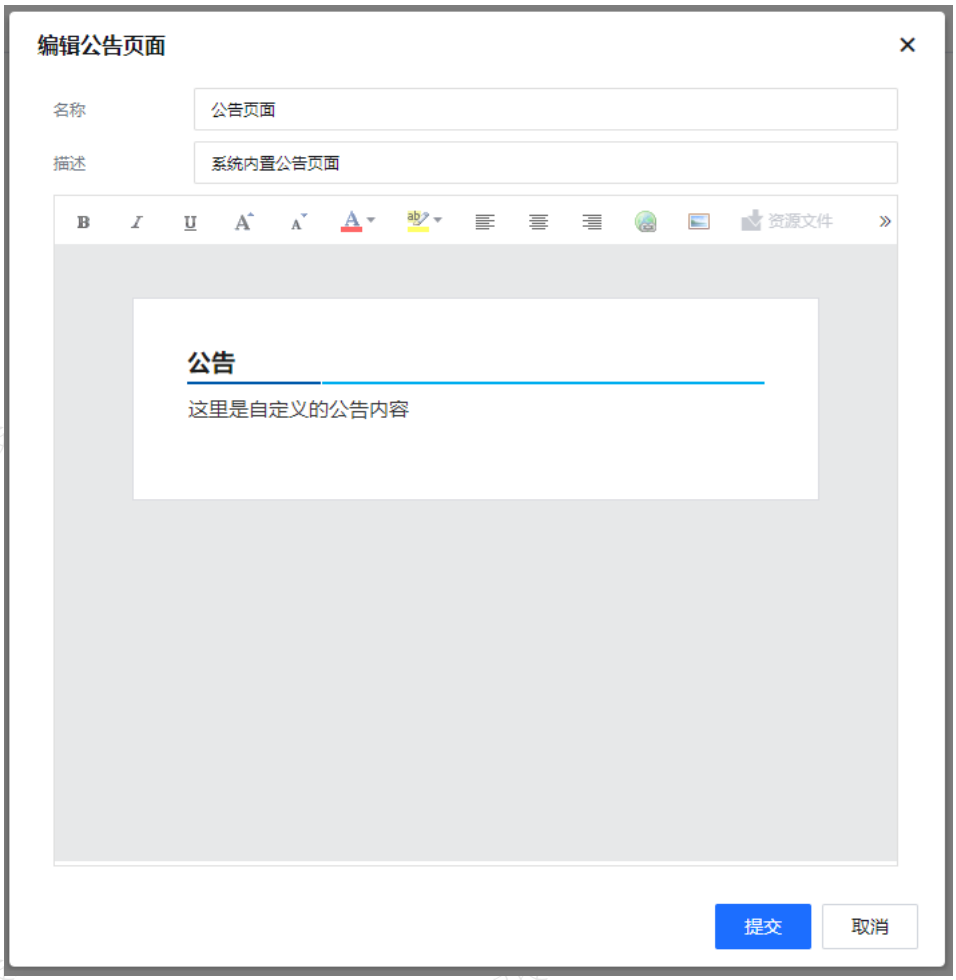
公告页面

公告页面可以新增、查看、复制、删除、刷新等操作，其中点击新增一个文件打开需要点击<上传页面>来上传对象，并在页面编辑中将相应的图片和JavaScript代码进行修改，修改之后上传ZIP包来配置(上传的文件名不支持中文)；点击<复制>可以复制当前用户自定义的页面，然后进行修改为其他公告页面；点击<下载>

可以下载自定义页面模版；点击<查看>可以预览当前用户自定义的页面。



公告页面点击公告页面名称，弹出编辑公告页面，如下图。



编辑公告页面：通过更改网页源代码来改变显示的页面，建议只改变文字和图片部分，其它的修改可能会导致页面上一些正常的链接丢失。

点击[资源文件]用户可以上传页面定制中显示的图片，图片只支持jpg和gif格式，

点击[恢复到默认]可以恢复到设备初始的页面

点击  按钮，显示代码视图，以代码显示展现文本。点击  按钮，可以全屏显示自定义公告页面。点击<提交>可以保存用户当前自定义的页面。

其他页面

其他页面包括：禁止访问页面、发现病毒页面、上网超时页面、网络准入客户端页面、上网时长提醒页面、

上网流量提醒页面、日流量配额页面、月流量配额页面、流速超限提醒、用户冻结提示页面、强制单点登录提示页面、防共享上网提示页面、移动终端拒绝提示页面，界面如下。

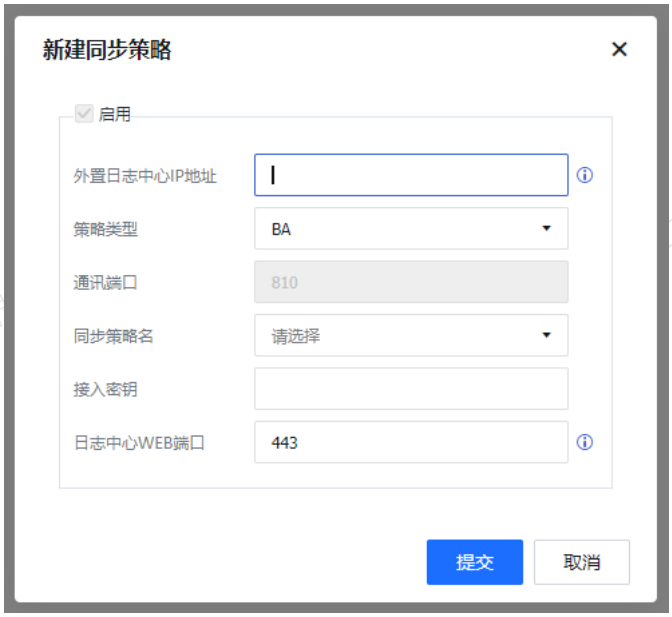
其他页面不能进行再进行新增页面策略，但是能进行编辑和查看操作，管理员可点击需要编辑的页面名称，可以编辑代理策略的名称和内容。

日志中心配置

日志中心配置用于设置外置日志中心和内置日志中心相关信息。外置日志中心包含服务器信息，内置日志中心包含自动删除日志相关选项。

外置日志中心同步选项用于设置外置日志中心IP地址、同步策略名、同步密钥、日志中心WEB端口信息。

1. 点击“测试链接”可测试设备与数据中心服务器的连通性。
2. 点击“同步”，设备会发送立即同步指令到数据中心服务器，进行日志数据的同步操作。
3. 点击<进入外置日志中心>进入外置日志中心WEB服务界面，用户名/密码默认是：admin/admin。
4. 点击<新增>跳转到新建同步策略界面，新增日志数据中心服务器。



- **外置日志中心IP地址：填写需要安装外置日志中心的服务器地址。（支持IP或域名的方式，填写域名时必须保证设备能够正确解析对应域名）。**
- **策略类型：可选BA（外置数据中心）或DLA（数据库）。**

• 同步策略名接入密钥：填写外置数据日志设置的同步账号的信息。

• 日志中心WEB端口：用于设置外置日志中心提供WEB服务的端口。

配置完成，点击<提交>。

内置日志中心日志选项：用于设置磁盘告警参数及自动删除日志的参数。

磁盘预警选项可设置日志保存太难书和审计日志持平预警百分比，当开启磁盘空间预计需要到告警选项中配置“磁盘空间告警”，当设备磁盘空间达到预警时会告知设备。

• 期望保留天数：推荐设置为180天（为了满足审计和法律法规等要求）。

• 自动删除选项：限制访问控制日志最大占用审计日志磁盘比例，超过该比例将自动删除最早一天的访问控制日志。

• 管理员可设置占用审计日志磁盘空间的百分比。

• 管理员启用自动删除最大保留天数功能，可以根据需求进行设置保留天数。

勾选关闭内置数据中心，以减少设备的资源消耗，提高日志记录性能，用于日志量比较大的时候，为了保证设备能记录完整的日志，不产生遗漏，勾选此项提高审计性能。

说明：

1．勾选关闭内置数据中心，设备还会占用磁盘空间，但是不会进行审计分析。

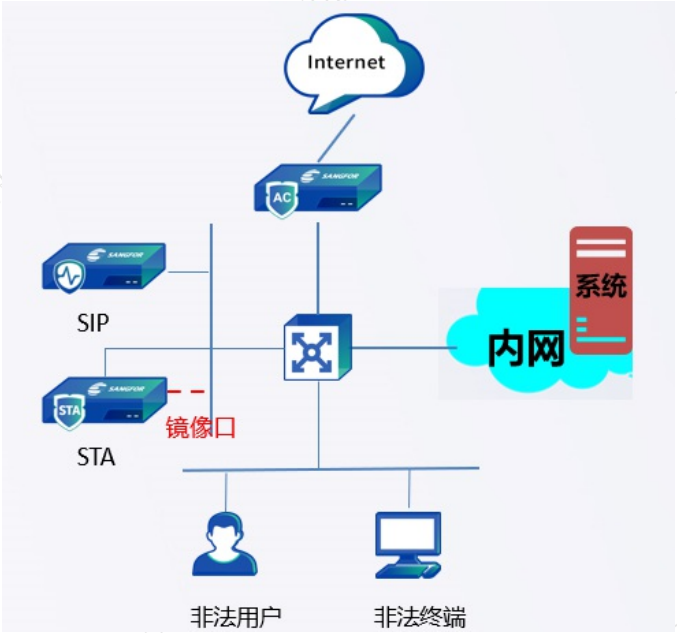
2．设备内存有限，建议安装外置数据中心。

深信服设备对接

深信服设备对接支持很多产品之间的联动，如AC对接SIP，支持用户信息同步、支持策略控制（在SIP设备能够下发冻结用户和上网提醒策略到AC，联动处置发现异常安全事件终端。支持对接SIP上报资产信息和在线用户信息，可根据IP上报指定的SIP设备或上报所有对接成功的设备。

当某企业同时购买了深信服的AC和SIP设备，希望和做网关的AC设备联动处置发现安全事件的终端。拓扑如下所示。

1. 实名制：同步用户信息到SIP；
2. 上网提醒：提醒发现主机有被攻击，及时遵照安全建议进行处置；
3. 冻结账号：发现疑似僵尸主机，一直在恶意外发，冻结账号。



对接过程：

1. 内网用户在AC实名制认证获取上网权限；
2. STA镜像内网、上网数据做安全监控；
3. SIP分析安全事件；
4. AC联动SIP，同步用户认证信息到SIP；
5. 发现安全事件，SIP联动AC下发策略实现对终端的处置。

预制条件

1. AC和SIP可以通信，需要开放端口TCP9998。
2. 开放端口：开放端口的目的是为了后面配置联动处置。

说明：

1. 如果AC设备是路由模式部署，SIP设备部署在AC的wan口方向，需要开放TCP9998端口（[系统配置/网络配置/高级配置/WAN口开放端口]）。

2. 如果是网桥模式或旁路模式则不需要此项配置，网络中放通AC到SIP之间的TCP9998端口即可。

操作步骤

步骤1.**AC设备配置。**设备在联网的前提条件下，配置[接入管理/接入认证/PORTAL认证/单点登录/深信服设备]，“转发认证信息到其他深信服设备”，配置转发策略和共享密钥。

步骤2.接入设置：[系统管理/系统配置/深信服设备对接]，启用深信服设备对接功能，支持两种对接方式，以下以手动配置为例。

- 自协商
- 手动配置

a)如果环境中AC数量比较少，可以随意选择对接方式；

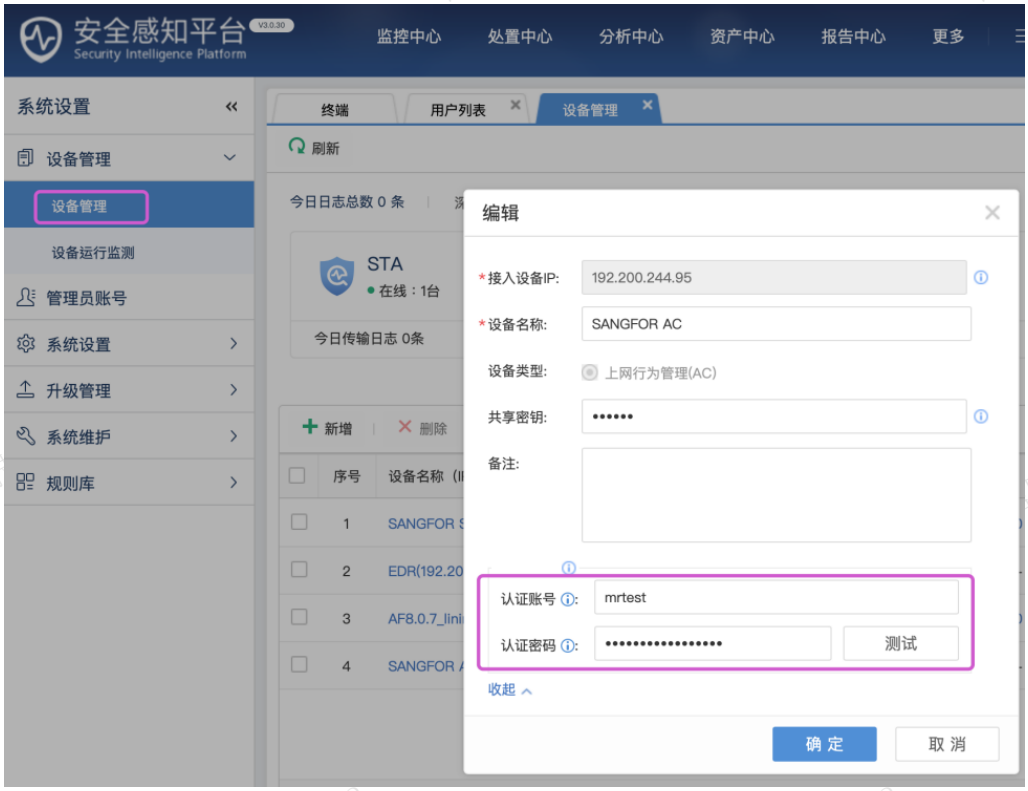
b)如果环境中AC数量比较多，可以选择自协商的方式，减少配置；

c)如果环境中有多台SIP设备，建议选择“手动配置共享密钥”方式，避免协商错误。

步骤3.**SIP设备配置**。在admin账号下拉列表中的[系统配置/设备管理]，新增上网行为管理设备，配置接入AC设备的IP和共享密钥；

步骤4.联动AC，配置认证账号和认证密码。

- 自协商方式，完成第一步用户信息同步配置后，无其他配置
- 手动方式，完成第一步用户信息同步配置后，配置高级选项，认证账号和密码和AC填写一致。



步骤5.接下来进行SIP设备配置，在[系统配置/设备管理]，新增上网行为管理设备，配置接入设备的ACIP和共享密钥。

步骤6.完成配置后，在[资产中心/主机资产]，可以看到用户信息。

步骤7.如果用户信息没有同步，可以点击“立即同步”进行手动同步操作。

说明

：

点击“立即同步”可以从AC设备立即同步用户信息，并更新到SIP平台，但是SIP原有的用户信息数据不会被清除。

步骤8.AC与SIP设备联动成功，深信服设备对接查看到对接设备的信息。

步骤9.SIP与AC设备联动成功，可在设备管理页面查看到对接设备的信息。

步骤10.效果呈现

5. 上网提醒

风险终端页面点击单个IP进行联动或者在[更多/联动AC界面]，进行新增时，上网提醒的提醒信息可以使用

系统推荐，也可也使用自定义。

6. 冻结账号

（1）在失陷主机页面与风险终端 二级页面联动AC。

（2）同时支持在更多->联动响应->联动AC页面新增。

高级配置

高级配置用于设置设备的一些其它系统配置，包括WebUI选项、代理服务器设置、远程维护、外部Syslog设置、加入集中管理设置、设备名称设置、证书生成、使用重定向和代理高级配置、SNMP设置、Radius认证服务器、DNS服务、开放接口、其他配置选项和SNAT代理上网高级配置。

WebUI选项

WebUI选项可以设置设备界面的一些常用的配置。包括默认编码、全局流速单位、流速单位进制、HTTPS登录端口、控制超时、控制台SSL证书颁发给、点击下载证书、控制台使用自定义SSL证书，配置界面如下所示。

- **默认编码：可以设置当监控到的数据编码，默认编码是GBK和BIG5。**
- **全局流速单位：可以设置监控到的网络流量的计量单位。**
- **流速单位进制：可以设置流速单位的转换进制，有1000进制和1024进制。**
- **HTTPS登录端口：可以设置登录控制台的端口，默认是TCP 443端口。**
- **控制超时：可以设置控制台超时的时间，在设定时间内控制台无操作，系统会自动断开连接，设备最大超时时间为10分钟。**
- **登录允许尝试次数：登录设备控制台输入账号密码错误，（尝试次数范围1-90次）。**
- **控制台SSL证书颁发给：设置的是登录控制台界面的SSL证书颁发给指定的IP或域名。**

• 点击<下载证书>，下载的是控制台界面的SSL证书，电脑安装好该证书，就可以去除登录控制台界面时的SSL证书告警框。

• 控制台使用自定义SSL证书：可以启用并上传自定义SSL证书，去除登录控制台界面时的SSL证书告警。适用于企业内部已经存在CA证书中心，管理员电脑已安装CA的根证书，AC设备创建证书请求，由CA证书中心为AC颁发服务器证书，最后将颁发的服务器证书（包含公钥和私钥）上传至AC。

点击<提交>，保存配置生效。

代理服务器设置

当用户需要通过代理的方式上网时，用户所有的数据都会发往代理服务器，而防火墙模块是通过检查目的地址和端口是否要拒绝该链接，会使得功能失效。要使得防火墙功能模块有效，需要正确识别代理服务器的数据真实链接的目的地址和端口，给防火墙功能模块提供地址和端口。

代理服务器设置设备默认情况下会对所有的代理数据进行检测，如果需要对固定的某台代理服务器数据进行检测，则在代理服务器设置中进行设置，在输入框内填入代理服务器IP地址或IP地址范围。

说明：

如果列表为空，则对发往任何地址的数据都会进行代理数据的识别，这样影响设备处理效率，建议在地址列表中填入代理服务器的IP地址。

需要保障设备能联网。

远程维护

远程维护用于设置是否允许从外网口远程登录设备，以及自动上报未识别URL、系统错误、未知应用信息和技术支持协助。其中包括升级维护、SSH维护、启用远程维护、启用未识别URL自动上传、启用系统错误自动报告、启用未知应用信息自动上报等。

• 升级维护：当设备需要进行升级的时候勾选，分别为：启用LAN/DMZ口访问和启用WAN口访问。启用WAN口时，默认24小时后关闭。

• SSH维护：当设备需要进行SSH维护时勾选，分别为：启用LAN/DMZ口访问和启用WAN口访问。启用WAN口时，默认24小时后关闭。

• 启用远程维护：用于设置是否允许从外网口远程登录设备，可设置启用24小时和长期启用。

• 启用未识别URL自动上传：启用后会将无法通过URL内置库识别的URL自动报告给深信服，用于丰富URL内置库，提供更好的服务，该功能不会泄露公司的使用信息。

• 启用系统错误自动报告：启用后会将系统错误信息自动报告给深信服，便于提供更好的服务，该功能不会泄露公司的使用信息。

• 启用未知应用信息自动上传：启用后会将未识别的应用自动报告给，便于提供更好的服务，该功能不会泄露公司的使用信息。

• 启用升级客户端，点击启用后才能通过升级客户端连接设备，不启用此功能设备无法连接升级客户端，该功能结合升级维护使用。

点击<下载黑匣子>选择下载最近1~30天的黑匣子。

点击<提交>保存配置才会生效。

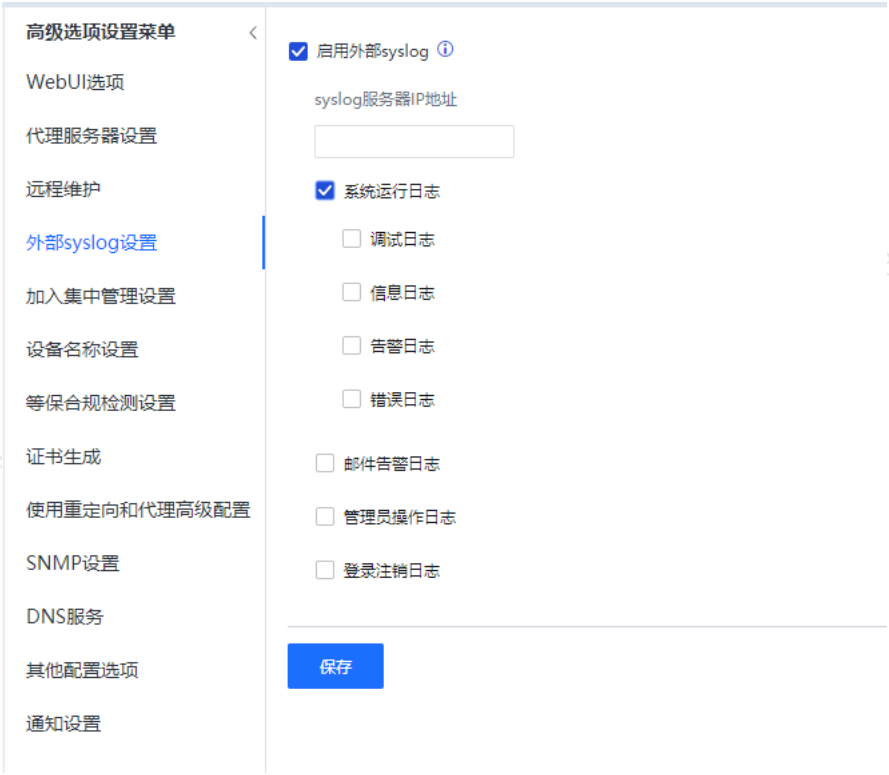
说明 ：

1.正常使用不需要进行调试和排障和升级设备，不建议启用WAN口访问功能，会导致设备存在风险。

2.当需要升级设备时，需要根据实际情况开启升级维护和启用升级客户端，设备才能连接到升级客户端进行升级操作。

外部Syslog设置

外部Syslog设置用于将设备上的系统运行日志、邮件告警日志和管理员操作日志同步到Syslog服务器上。必须要启用外部syslog服务器，此功能才生效。



- **Syslog服务器IP地址：用于设置Syslog服务器的IP地址。**
- **系统运行日志：可以设置将调试日志、信息日志、告警日志、错误日志等同步到Syslog服务器上。**
- **邮件告警日志：当勾选邮件告警日志会将该日志同步到syslog服务器上，配置的邮件地址确保能正常收发邮件，详情配置请参考告警选项章节。**
- **管理员操作日志：设备会将管理员操作日志同步到syslog服务器上**
- **登录注销日志：设备会将登录注销日志同步到syslog服务器上。**

加入集中管理设置

加入集中管理用于设置AC设备是否加入集中管理进行受控，加入后管理员可以对该设备下发策略，并且受控端的权限也可以由中心端下发。设备支持加入BBC集中管控或X-Central（云图）集中管控。

接入BBC配置：

• 解除集中管理：用于加入集中管理后，输入密码进行解控。该密码由中心端管理员掌控。此处选项为灰色说明未连入中心端。

• 中心端接入地址：用于设置连接集中管理的设备。该地址由中心端管理员掌控。

• 点击<测试有效性>，检测IP和端口号是否可以通。

• 接入设备名称：填写接入集中管理中心端的用户名。

• 勾选<同步修改本地设备名称>：本地受控制端的设备名称将同步终端里面设置的设备名称。

• 接入密码：填写接入集中管理中心端的密码。

接入X-Central配置：

• 企业ID：填写X-Central的企业ID。

• 接入设备名称：填写接入集中管理中心端的用户名。

• 勾选<同步修改本地设备名>本地受控端的设备名称将同步终端里面设置的设备名称。

• 接入密码：填写接入集中管理中心端的密码。

在接入集中管理时，中心端下发的配置，在受控端不能编辑和删除。

设备名称：用于设置设备的名称，当有多台设备加入中心端时，可以通过设备名称区分受控端设备，或者当有多台设备使用同一账号同步数据到外置数据中心时，用于区分同步数据的设备。

如果原先未设置设备名称，加入集中管理后，自动将集中管理帐户作为设备名称。

证书生成

证书生成是加入集中管理中心端的时候使用。

使用重定向和代理高级配置

当设备是网桥模式部署时才会有此功能，启用模式部署不会出现此功能。

当网桥IP和终端不能通信的情况下，设备WEB认证、准入、代理检测等重定向功能需要与内网电脑通信，默认可以通过虚拟IP支持。

重定向和代理高级配置的设置包括重定向、代理、虚拟地址。

1. **重定向**：包括认证重定向，拒绝重定向等。

勾选启用强制根据目的地址路由，选择重定向包发送网口。开启后设备发出的重定向包会查询路由规则选择出口，系统默认是按照WIWO（哪个口进哪个口出）方式发送重定向包。

2. **代理**：包括邮件代理和SSL代理等。

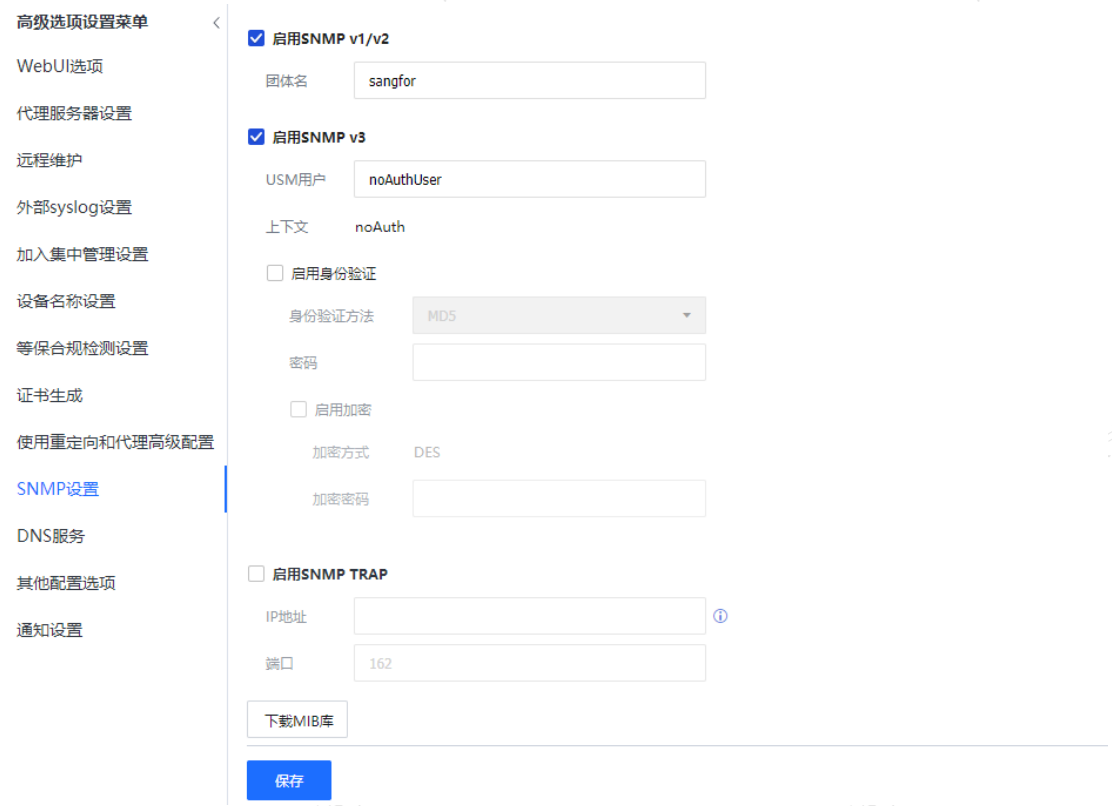
• 勾选启用强制根据目的地址路由：选择代理数据发送网口。开启后设备发出的代理数据包会查询路由规则选择出口，系统默认是按照WIWO（哪个口进哪个口出）方式发送代理数据包。

• 关闭地址还原：在开启强制根据目的地址路由，选择代理数据发送网口后，关闭地址还原功能。网桥模式下的代理地址还原功能默认开启，路由模式不支持地址还原功能。

3. 虚拟地址：可配置虚拟IPV4地址和虚拟IPv6地址。是指客户端重定向后的IP地址是一个虚拟IP地址。

SNMP设置

SNMP设置是开启设备的SNMP功能，如下图所示。



- 启用**SNMP v1/v2**：开启**SNMP V1/V2**版本，设置团体名。**SNMP**客户端可根据设置的团体名查看设备的运行情况。
- 启用**SNMP v3**：开启**SNMP V3**版本。设置**USM**用户名。
- 启用身份认证：开启和设置身份认证方式，可以选择**MD5**和**SHA**。
- 启用加密：开启**DES**加密方式，设置加密密码。
- 启用**Snmp trap**：**Snmp trap**告警功能，配置**Snmp**服务器**IP**和端口。

说明：

必须启用Snmp v1/v2或Snmp v3任意一种，无法单独使用。

下载MIB库：点击可下载设备的MIB库，导入到SNMP管理软件中，从而通过管理软件对设备的各个参数进行监控。

等保合规检查配置

基于等级保护基本要求，为了确保设备的安全策略、基线配置符合合规要求。可对接深信服合规自检平台的中心端对AC设备当前配置状态进行自动化检查，解决了人工核查效率低、检出率低等问题，辅助管理人员快速识别问题、快速优化整改，有效满足测评的要求。

- 启用等保合规检测：启用等保合规检测服务；
- 设备类型：选择等保合规检测中心端设备类型；
- 中心端IP：填写等保合规检测中心端设备的IP地址；
- 中心端端口：填写等保合规检测中心端的端口，与中心端的配置保持一致；
- 当前设备IP：填写当前设备的IP地址，用于校验。

DNS服务

DNS服务器功能，如果需要使用AC作为DNS服务器，即PC的DNS服务器指向本机设备，则需要开启此功能。

SNAT代理上网高级配置

当设备需要进行SNAT代理上网时，选择启用源端口绑定，点击<提交>即可生效。

其他配置选项

管理员可设置VPN接口所属区域、应用识别设置、隐私设置和查看设备的日志。

VPN接口所属区域包括LAN区和WAN区。

• LAN区：表示VPNTUN默认属于LAN区域。

• WAN区：选择此选项表示经过VPNTUN口的数据都被当成LAN->WAN数据，要求被认证和审计、流控等。

通知设置

通知设置功能支持短信通知服务器和邮件通知服务器。

短信通知服务器

短信通知服务器的主要功能：

• 验证码通知：短信认证发送短信验证码。

• 自注册审批：发送审批通过和审批不通过的消息。

• 新终端审批通知：用户使用新终端登录，将使用该处的短信平台通知管理员审批。

短信通知服务的类型包括中国移动、中国联通、中国电信、HTTP协议、外部服务器短信模块。短信通知服务器管理包括新增和删除服务器，启用和禁用的操作，以及短信通知模板的设置。目前常用HTTPS协议作为短信通知服务器，详细操作请参考接入认证的短信认证章节。

邮件通知服务器

当设备中配置邮件通知服务器发送邮件服务器支持加密的邮箱进行告警。主要作用有

通知内容支持邮件认证验证码通知、自注册审批通知。

操作步骤

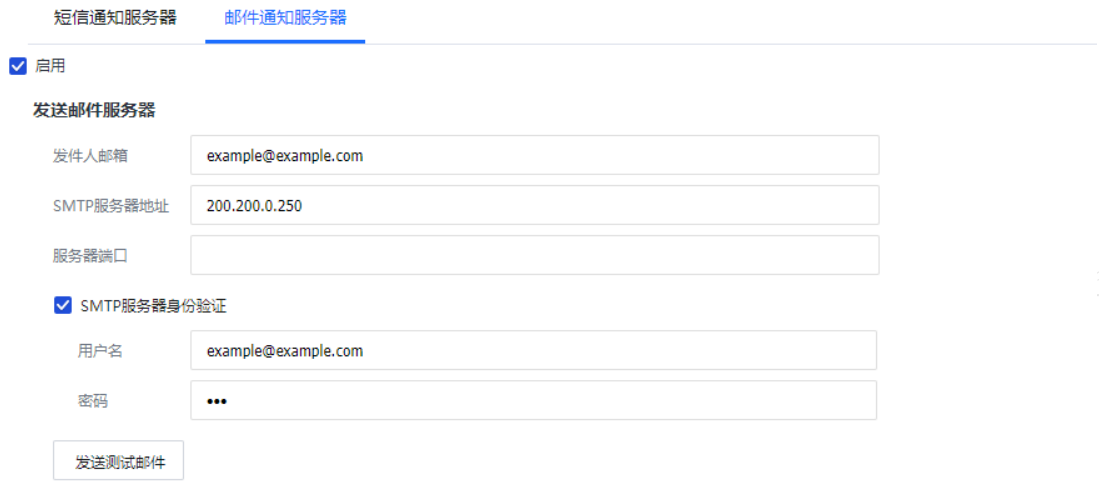
步骤1.设置告警邮件的发送邮箱服务器地址和接收邮箱，先配置收件地址邮箱，确保该邮箱能正常接收邮件。

步骤2.例如配置QQ邮箱服务器，需要在[设置/账号]找到服务器配置方式，确保SMTP已开启。根据需求点击<如何使用 Foxmail 等软件收发邮件？>、去获取STMP服务器地址和端口。

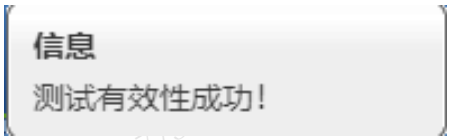
步骤3.点击<生成授权码>，跳转验证码发送页面，使用绑定邮箱的手机号发送短信到指定的号码，手机上发送成功，再点击<我已发送>。

步骤4.页面弹出生成授权码。

步骤5.点击<配置发送邮件服务器>跳转到邮件服务器通知页面。填写刚才配置的邮箱地址、SMTP服务器地址、服务器端口。STMP服务器验证填写的用户名与发件邮箱一致，密码为授权码。



步骤6.点击<发送测试邮件>，输入能正常接收邮件的邮箱地址，发送成功后，页面会弹出“测试有效性成功”，说明配置的发送邮件服务器能正常发送邮件。点击<提交>邮件通知服务器配置完成。



系统诊断

系统诊断功能包括：系统日志、抓包工具、命令控制台、上网排除故障、重启操作、设备健康检查等功能。

上网故障排除

当用户上网的流量经过AC设备出现异常时，可通过AC的上网故障排除功能查询该用户的数据包在通过AC设备时被拒绝的原因，便于快速定位故障原因。上网故障排除页面提供[直通排障]和[设备搬包]（搬包功能仅路由和网桥模式下可使用）两种故障排除手段。

直通排障

直通排障一般用于测试上网异常IP是否由AC设备拦截造成。针对上网异常的IP开启直通后，如果AC相关功

能模块对该IP进行了拦截阻断，则会在直通日志终打印出被拦截的原因以及对应的功能模块，管理员可根据直通日志可快速定位问题。

设备上架时为了避免影响业务，可以开启直通，当出现终端异常断网的情况下，可以通过直通排障的日志快速定位问题并恢复业务。

点击<设置并开启>，出现设置开启条件界面，可设置各种过滤条件，包括[拦截日志过滤条件]和[同时开启数据直通]，如下图。

拦截日志过滤条件：用于设置对指定的IP地址开启拒绝列表，默认包括所有网段。

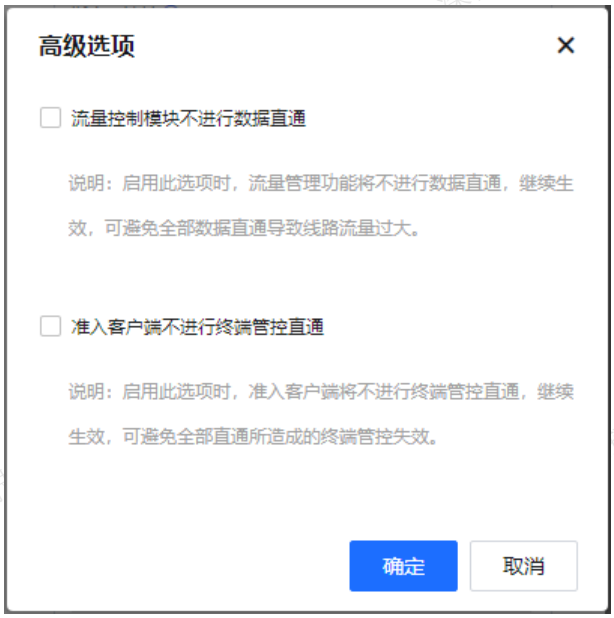
点击<协议条件>，可根据协议类型和端口范围过滤拦截日志，如下图。

协议类型可选择：所有、TCP、UDP、ICMP和其他五种类型。

勾选[提高拦截日志的可读性]，将通过中文显示拦截日志；如果此项不勾选，则通过英文显示拦截日志。

勾选[同时开启数据直通]，可设置开启直通的IP地址或者地址段。此时对于这些IP地址设置的上网策略将不生效，原本策略设置拒绝的数据包会被设备放行。

点击<高级选项>，可设置对流量控制模块和准入客户端策略是否开启直通。如果勾选<流量控制模块不进行数据直通>，则流量管理策略仍然生效，可以避免由于全部数据直通导致流量过大，对用户上网环境造成影响；如果不勾选，流量管理策略将不生效，用于定位被流量控制模块拦截的情况。如果勾选<准入客户端不进行终端管控直通>，则已下发到终端的准入策略（基于准入客户端的策略）仍然生效，可以避免终端安全基线检查失效，终端管控失效；如果不勾选，下发到终端的准入策略不生效，用于定位被准入模块拦截的情况。



当前操作状态：将显示直通和拦截日志的开启情况，如下图。

点击<关闭>，关闭拦截日志和直通。点击<立即刷新>查看拦截日志，数据包被拦截的情况，如下图。

序号	时间	源->目标	协议	设备	大小	线路	应用名称	应用规则	源	丢包标记	动作
1	18:15:42	11.11.11.34:4607 -> 100.1	tcp	eth2 -> NULL	54(B)	线路1	自定义应用_自定...	公司邮件	authv	DROPFL...	Auth policy logic(Acode) dropped
2	18:15:42	100.100.24.200:80 -> 11.1	tcp	eth0 -> NULL	66(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) throw
3	18:15:39	11.11.11.21:4620 -> 100.1	tcp	eth2 -> NULL	54(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) dropped
4	18:15:39	100.100.24.201:443 -> 11.	tcp	eth0 -> NULL	54(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) dropped
5	18:15:31	11.11.11.34:4607 -> 100.1	tcp	eth2 -> NULL	54(B)	线路1	自定义应用_自定...	公司邮件	authv	DROPFL...	Auth policy logic(Acode) dropped
6	18:15:31	100.100.24.204:80 -> 11.1	tcp	eth2 -> NULL	54(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) dropped
7	18:15:31	11.11.11.30:4616 -> 100.1	tcp	eth2 -> eth0	54(B)	线路1	0	0	web aut...	DROPFL...	(line:760)this packet had been dropped
8	18:15:31	11.11.11.30:4616 -> 100.1	tcp	eth2 -> NULL	54(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) dropped
9	18:15:26	11.11.11.30:4616 -> 100.1	tcp	eth2 -> NULL	54(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) dropped
10	18:15:26	11.11.11.24:4617 -> 100.1	tcp	eth2 -> NULL	1514(B)	线路1	自定义应用_自定...	公司邮件	authv	DROPFL...	Auth policy logic(Acode) dropped

说明：

1．拦截日志和直通功能开启后，如果管理员未手动点击<关闭>，即使设备重启，仍然是开启状态。

2．审计策略在开启直通也依旧生效。

设备搬包

搬包功能是AC设备在路由模式和网桥模式下提供的一种紧急逃生的能力，当设备功能模块异常影响业务时，可通过搬包功能直接放开对流量的流量的控制从而保证业务流量不中断。

AC设备开启搬包时CPU、内存、IO等资源占用将大幅降低，经过AC设备的数据会被直接转发，不再受任何策略影响(认证策略、访问权限策略、流控策略、上网审计策略等)。

与直通、全局排除功能相比，搬包生效时所有数据包会被直接转发，不会匹配任何策略逻辑，不会生成任何策略管控日志，搬包是一种更彻底的流量放通机制。

在开启搬包功能时，可以选择对所有流量进行搬包，也可以对指定条件的流量进行搬包（如下图所示）。

说明：

1、必需由设备处理的核心逻辑不受搬包影响，具体为：源地址转换(NAT代理上网)、目的地址转换(端口映射)、代理上网流量转发(上网代理)、路由转发；

3、部分特殊流量不支持搬包，如：广播包、组播包；

4、开启搬包时，开启功能前已存在的连接不支持被搬包，这部分连接将继续受策略管控；

5、关闭搬包时，关闭功能前已在搬包的连接不支持退出搬包状态，搬包状态将持续到连接销毁；

6、子连接将会直接继承父连接的搬包控制状态，即父连接被搬包则其对应的子连接也会被搬包，反之父连接没有被搬包其对应的子连接也不会被搬包；

7、开启搬包后，会出现客户端自动找网关失败、客户端获取准入策略失败、防Dos攻击拦截异常等情况。

故障监控中心

在[系统管理/系统诊断/故障监控中心]里有网络故障排查、用户认证故障排查、客户端解密故障排查、权限策略故障排查、web访问质量监测和单用户检测六个部分。用于帮助运维人员、技术支持工程师等专业人士进行故障自查。

网络故障排查

网络故障排除是用来监控网络的状态，当网络出现异常时，识别错误类型，并提供解决方案。目前可以识别4种网络异常。

1. [内网DOS攻击]

事件说明：内网DOS攻击事件xx次，攻击流量会导转发设备性能超限、线路拥塞，造成上网卡慢或者无法访问网络。

错误类型：内网DOS攻击。

解决方案：请检查网络拓扑变化，是否构成环路。请隔离对应IP设备并对该设备进行病毒查杀。

2. [网口丢包异常]

事件说明：网口丢包事件xx次，网口丢包、错误包会造成上网卡慢，影响用户上网体验。

错误类型：rx_crc_errors。

解决方案：该错误表明数据包传输物理层故障。请更换连接对应网口的网线，或者更换和网线直连的对端网口。

3. [ARP异常]

事件说明：ARP异常事件xx次，设备网关存在ARP无回复或回复异常。

错误类型：ARP异常。

解决方案：请检查网关设备的运行状态及连通性。

4. [网关PPS异常]

事件说明：设备PPS超限事件xx次，PPS造成设备所有控制和审计功能失效。

错误类型：网关PPS异常。

解决方案：设备持续PPS超限表明当前设备性能不足，建议对经过设备的流量进行分流，或者联系商务渠道更换更高端平台设备。

⚠ 注意：

AC以网桥模式部署时才支持网关PPS异常检测。

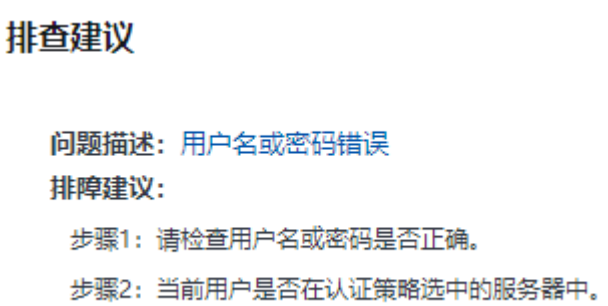
用户认证故障排查

管理员利用“用户认证故障排查”工具可以自查用户出现认证异常无法上网、上线错误等异常问题。在[用户

认证故障排查]界面可以查看设备记录的用户认证过程中出现的异常情况，方便运维人员快速定位问题。

管理员在输入框输入异常用户的用户名/IP/MAC地址，点击<搜索>，即可看到该用户认证过程中的异常情况。

管理员在排障建议列表点击<详情>能弹出排障建议。



管理员可查看问题描述：如“用户名或密码错误”，参考排障建议步骤去排查问题。

单用户检测

“单用户检测”工具包含[终端重定向检测]和[准入客户端日志检测]。

终端重定向检测

当整体网络质量判定不能解决问题时，可以对单用户进行针对性检测。

例如：在发现用户A的在上网慢的列表中，可以在单用户检测—检测对象中输入用户名或IP地址或者点击选择用户在下列组织结构中勾选用户。

1. 点击<选择用户>，在设备用户组织结构中选择指定用户。

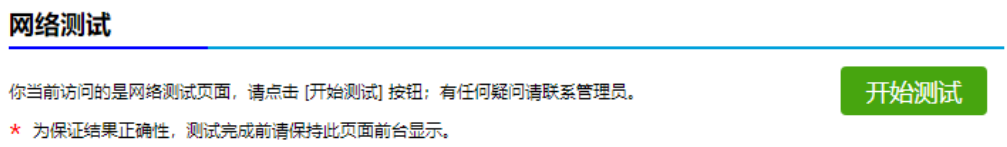
2. 确定<提交>后，在监测地址点击<设置>，设置监控地址。

3. 终端页面重定向：可以选择访问百度是重定向到测试页面或者所有web访问重定向到测试页面。

4. 监视地址：可以选择使用内置监测地址库或者自定义监测地址。

5. 确定<提交>后，点击开始设置，以www.baidu.com为例。

6. 用户访问www.baidu.com，重定向到测试页面。



7. 点击<开始测试>后，用户开始检测。测试时会有时间提示。

8. 管理员页面显示开始检测。

9. 用户检测完毕。

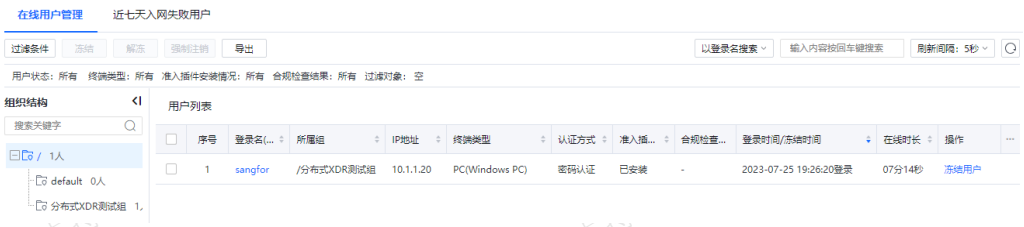
10. 管理员页面显示检测结果。

准入客户端日志检测

通过在Web控制台收集用户终端上的准入客户端日志，无需使用U盘、远程工具等方式从用户终端拷贝准入客户端日志，从而提高管理员排障效率。

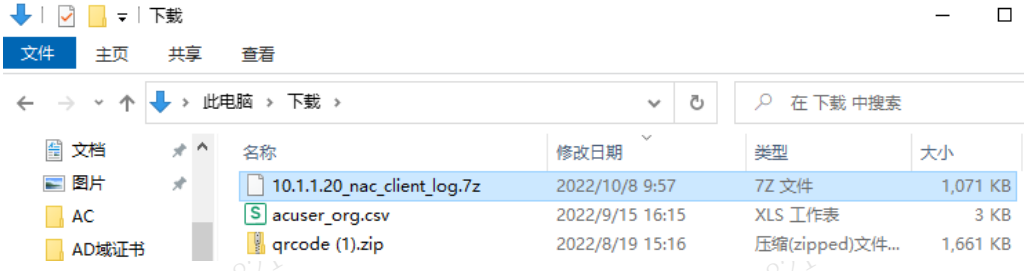
例如：企业部署了AC设备，为满足企业办公安全，配置了终端检查策略。当员工反馈终端PC异常，管理员无法只根据AC设备提供的准入安全日志定位问题时，需要结合终端PC上的准入客户端日志更深层次地分析、定位问题，可直接在AC设备Web控制台下载指定监测对象的准入客户端日志。

1. 在[全网监控/入网用户管理]查看员工信息，确认用户已上线，并安装准入插件。



2. 在[全网监控/故障监控中心/单用户检测]中的“准入客户端日志检测”工具填入监测对象IP，点击<下载日志>。

3. 下载完成后可在本地查看日志文件



客户端解密故障排查

客户端解密故障主要根据准入客户端的安装情况、证书安装情况、异常详情来定位故障信息。

其中排查思路如下：

• 匹配解密策略：若客户端解密故障排查中没有该用户信息或匹配解密策略为空，检查解密策略是否已经匹配且匹配正确。

• 准入客户端的安装情况：

未安装：该用户未安装准入客户端，检查终端准入客户端安装运行情况，可手动安装。

已安装：该用户已安装准入客户端。

• 证书情安装情况：

证书安装成功: 该用户已安装证书成功。

其他状态包括：系统证书安装失败、火狐证书安装失败、证书安装失败、证书无效、证书过期。

• 异常情况：

代理正常运行：状态正常。

代理异常：准入客户端代理无回包。

驱动异常：包括驱动文件不存在、驱动签名失效、驱动被杀毒软件阻止、基本筛选引擎（BPE）服务被禁止。

权限策略故障排查

通过“权限策略故障排查”可以查看用户访问权限策略匹配情况，当策略匹配的用户与实际期望不符合时，运维人员或工程师可以使用该功能进行排查。

管理员在输入框输入异常用户的IP地址，点击<开始监测>，可以看到该用户匹配到的所有策略。通过与实际需求进行比对，找到异常点并调整策略。

管理员可以在应用类型中选择需要查找的相应策略，点击<匹配详情>，可显示该IP 对应的策略名称、策略控制序号、匹配维度、匹配结果等信息，可根据这些信息找到异常点来调整策略信息。

解决方法：识别到该策略的DNS协议没有放通，导致访问所有的网站都拒绝，回到权限策略设置把DNS协议去掉勾选，就能访问正常。

Web访问质量监测

用于显示内网终端访问监测网站的网络质量。以 HTTP（默认所有网站）与HTTPS（用户自定义网站）请求作为网络质量检测的评估对象，对核心指标（RTT时延、DNS时延、TCP重传率..)进行抽样，根据质量分析数据模型来对所有上网IP进行质量评估，结果分两类：优、差，并按单用户的网络质量分布情况评估客户整体的网络质量，结果为差时将提供潜在问题分析建议。可以查看当前网络质量监测状态，近日网络质量，以及当前网络质量及网络诊断结果。

点击<质量定义>，用于设置检测网络实时质量定义设置。

统计网络质量的活跃用户少于N人数可以自定义填写。默认10人，允许输入1 - 100之间的数字。

全天质量查的定义：用于监测判断，当全天质量查的时间累积超过N分钟时，判断为网络质量差，默认30分钟，允许输入10 - 300之间的数字。

点击<选择日期>可以查看一周内的网络质量状态。

点击<监测对象>用来选择网络监测的网站。默认选择所有网站。用户也可以指定要监测的网站，最多可以有3个监测列表，每个列表最多100个域名。

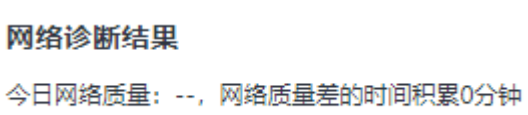
在检测对象下拉点击<管理>，进行编辑网站列表。

鼠标移到波形图上，出现悬浮框，可以看到详细的网络质量状态，当网络质量为差的时候，可以点击查看，进行查看上网慢用户列表。

纵坐标是统计到的在上网的用户个数，网络质量好的用户数+差的用户数。

鼠标移到波形图上，可以查看当前时间上网质量优和差的用户个数，点击<查看>可定位当前上网慢的用户列表。

网络诊断结果：用来查看详细的网络质量，可以显示若干条详细网络质量较差的原因。



可能存在的原因：

1. 未开启流控。
2. 带宽不足（如果当天存在连续10分钟http流量占带宽90%）。
3. P2P抢占带宽，建议限速，（如果当天连续10分钟p2p流量占带宽90%）。
4. 建议设置保证通道 （流控有丢包10%以上且未设保证通道）。
5. 策略（xxx）流控限制较低。
6. 策略（xxx）连接数限制较低。
7. DNS配置错误。
8. 提示内侧或外侧性能瓶颈。

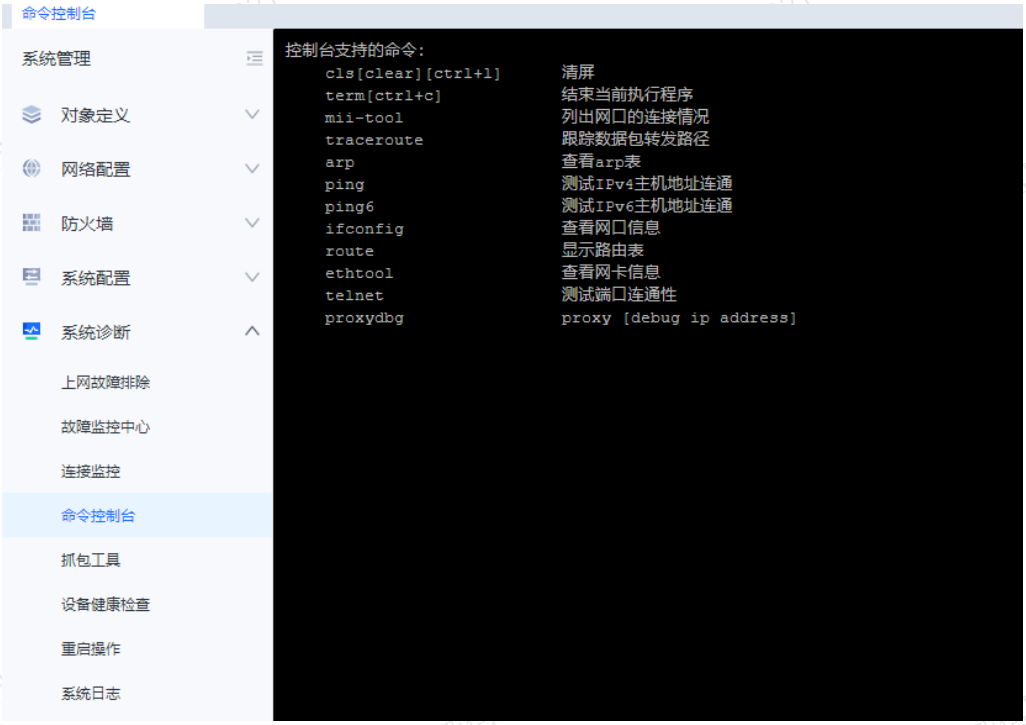
连接监控

连接监控是用于查看指定的用户或者IP的连接情况，可以通过IP地址和用户名来查询连接信息。

命令控制台

命令控制台提供一个简单的控制台命令行，可用于对设备的一些简单信息进行查看，支持的命令包括：arp（查看arp表）、mii-tool（列出网口的连接情况）、ifconfig（查看网口信息）、ping（测试主机地址连通）、telnet（测试端口连通性）、ethtool（查看网卡信息）、route（显示路由表）和traceroute（跟踪数据包转发路径），在命令行页面直接输入命令回车即可，如下图所示。

在命令行输入：network-monitor，会出现网安对接，可看到第三方的对接日志。

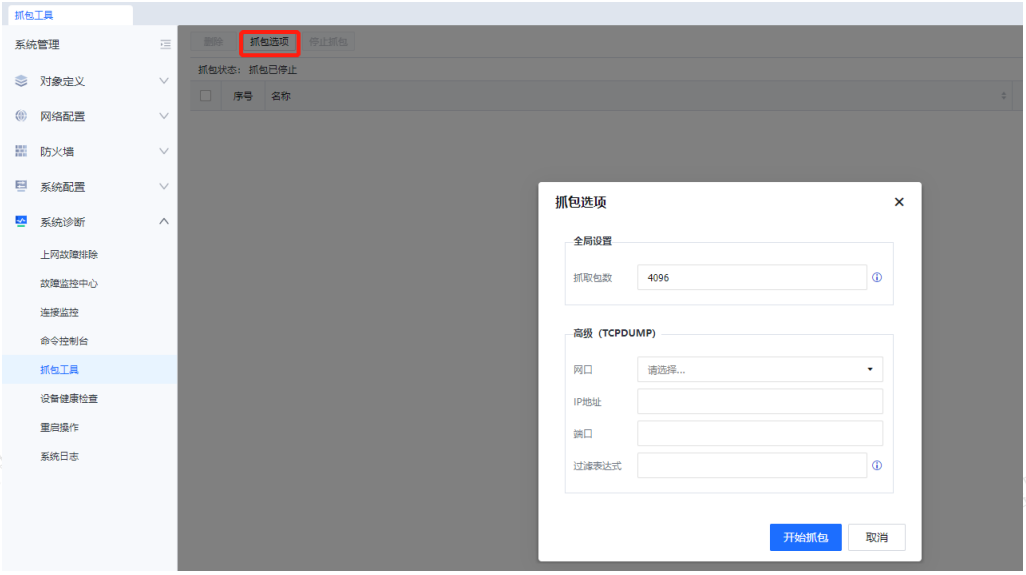


抓包工具

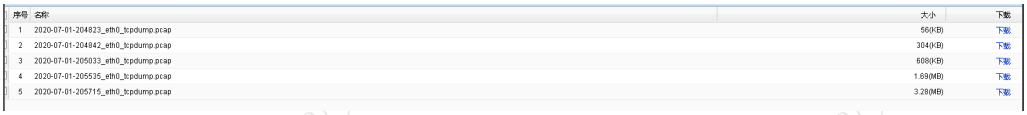
抓包工具用于对流量经过设备的数据包的分析，以便快速定位问题，可以作为排错的辅助工具，最大可抓1W个包，可以通过表达式[兼容tcpdump]增加参数条件。

例如：先在AC配置一台PC通过AC进行密码认证来上网。管理员可通过AC的抓包工具来抓包分析，PC地址是172.172.4.10，上网出口是eht0。

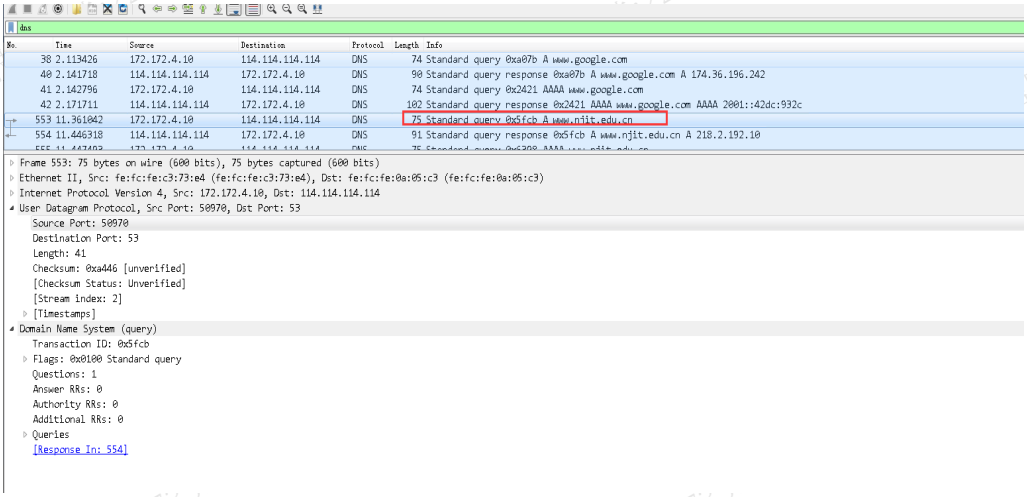
步骤1.在打开[系统管理/系统诊断/抓包工具]页面，点击<抓包选项>抓取包数，默认；网口选择eth0；IP地址：172.172.4.10；其他可不填。



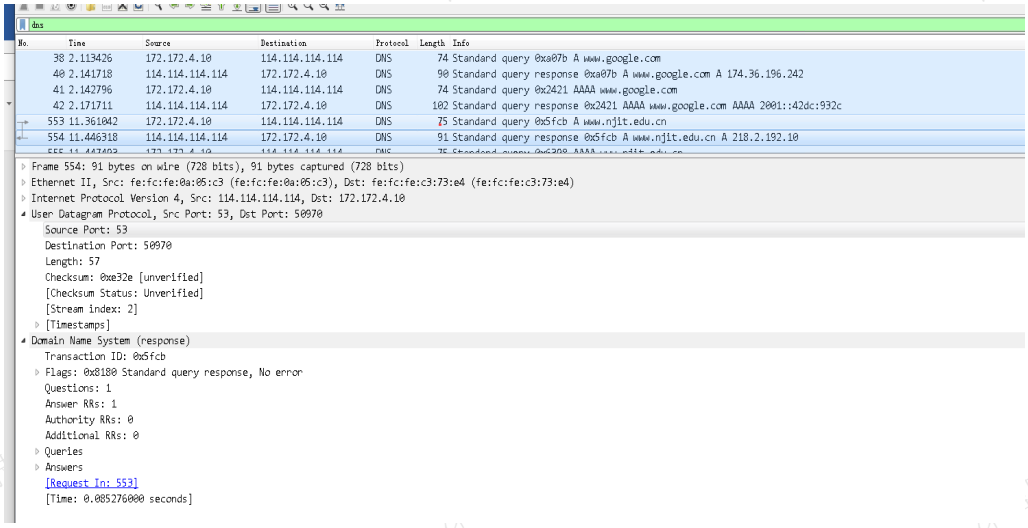
步骤2.先清除浏览器缓存，访问学校官网http://www.njit.edu.cn，然后输入AC登录名与密码进行认证，跳转到学校官网，回到AC控制台，可以看到抓取的数据包生成的pcap文件。



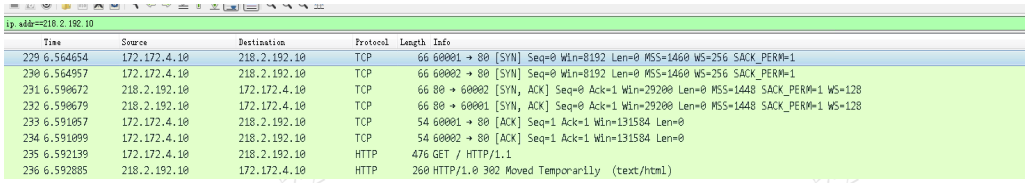
步骤3.使用wireshark打开该文件，开始分析，首先是PC向DNS服务器114.114.114.114发出DNS Query请求，请求www.njit.edu.cn的A记录。



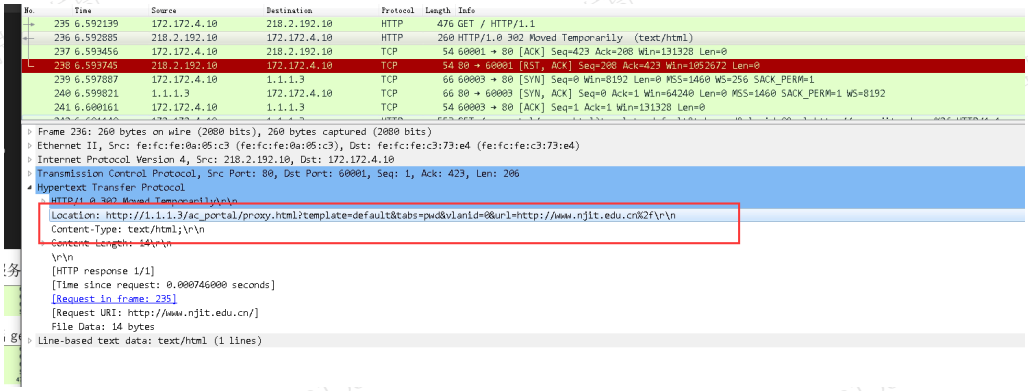
步骤4.DNS服务器114.114.114.114回复DNS Response，解析出www.njit.edu.cn域名对应的A记录



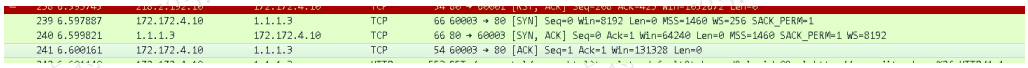
步骤5.PC向解析出的www.njit.edu.cn服务器地址发起tcp三次握手，PC向www.njit.edu.cn服务器发出get请求，请求主页。



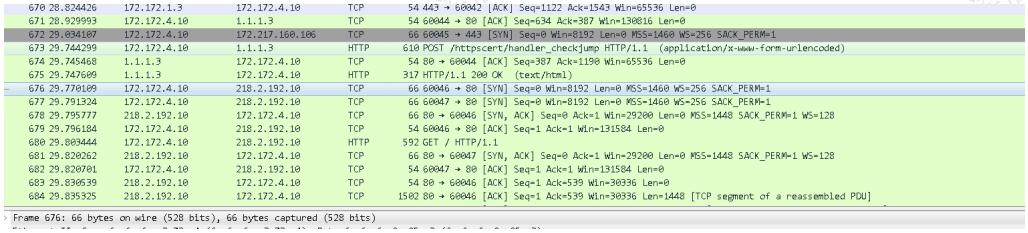
步骤6.请求被AC设备拦截，AC伪装成学校官网服务器，向PC发送302重定向报文，重定向到1.1.1.3 AC上网认证界面。



步骤7.然后PC向1.1.1.3发送TCP三次握手请求，握手建立成功后，向1.1.1.3发送get请求，请求认证界面。



步骤8.认证通过以后，PC可以正常访问网页。

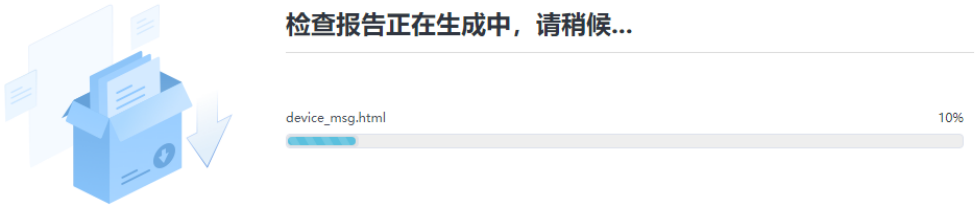


设备健康检查

可以对设备进行健康检查，包含硬件检查、系统软件检查以及管理合规检查，降低设备故障发的概率，发现重要业务潜在的业务风险，保障重要业务策略的匹配与有效，以及满足合规性要求。在[系统管理/系统诊断/

设备健康检查]选择<立即检查>进行设备健康检查。

设备健康检查报告生成中。



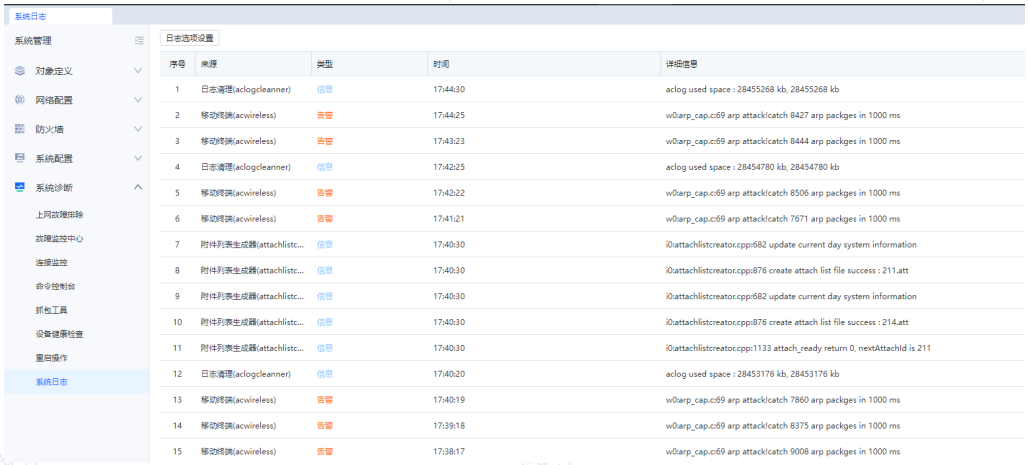
检查完成后，可以下载设备健康检查报告。

重启操作

管理员在[系统管理/系统诊断/重启操作]，提供设备重启网关和重启服务两个功能按钮。重启设备和网关设备都会断网和影响业务，请谨慎操作。

系统日志

系统日志用于查看设备各模块运行状态日志，可通过日志判断设备各模块是否正常运行，如下图。



日志分析平台

日志分析平台是基于原外置数据中心的架构，基于海量的上网日志，以多种应用商店为载体，提供多种行为感知应用来帮助解决日志分析的问题。提供日志中心、业务分析、带宽分析、办公网上网态势和未关机检测分析等应用体验。在首页的右上角点击<进入日志分析平台>可以跳转到日志分析平台首页。

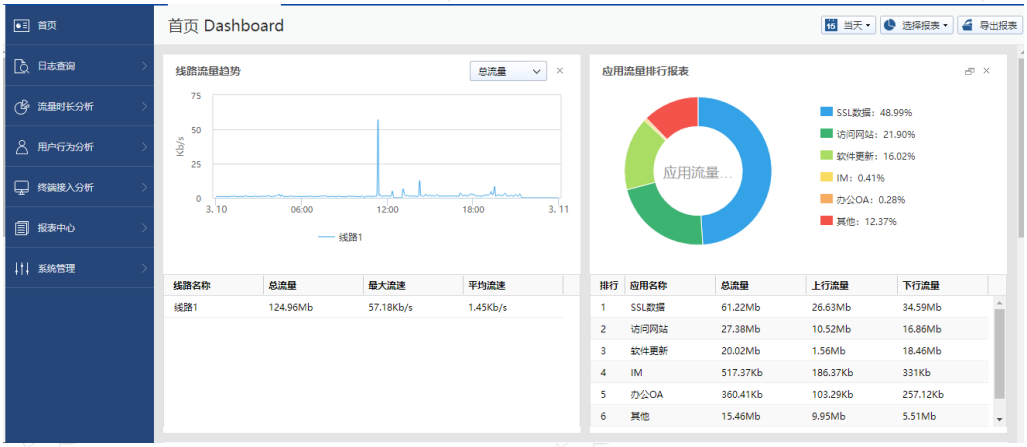
说明：

在查看日志之前需要根据先在AC上先配置相应的策略，如权限策略、行为审计策略等，

再进入日志分析平台才能查看到对应的日志。

日志中心

日志中心提供日志查询服务，可以查询到来自于AC设备的用户上网行为日志、用户上网流量日志、用户上网时长日志、移动终端接入日志等，跟AC设备的日志中心的日志保持一致。点击[我的应用/日志中心]图标可以快速进入日志中心。



日志查询

日志查询包括用户行为查询、终端接入日志、安全日志三个部分。

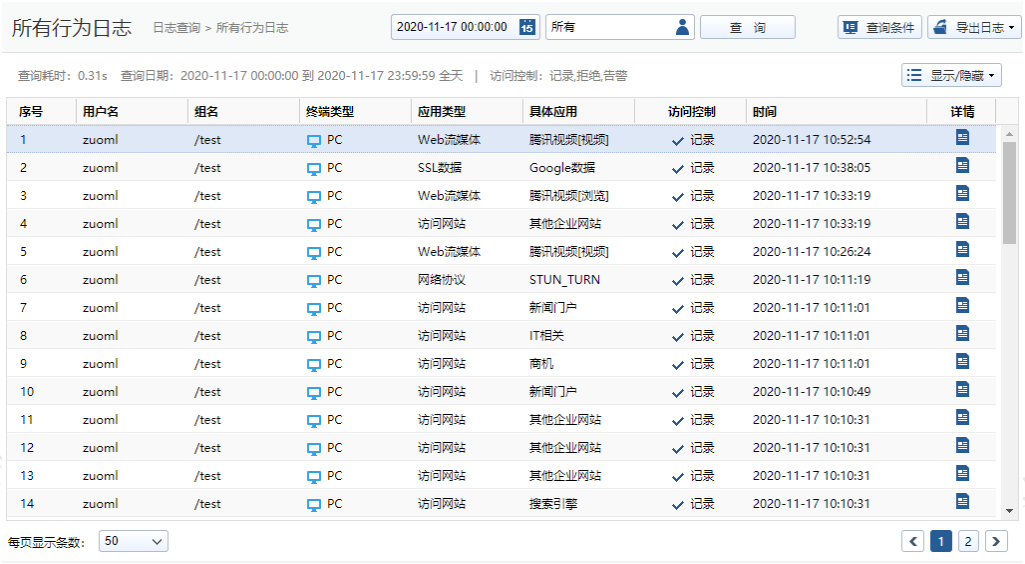
用户行为查询：包括所有上网行为、网站访问日志、文件审计日志、即时通讯日志、邮件收发日志、发帖/发微博日志、搜索关键字日志这几个部分是对具体的常见应用进行详细查询。

终端接入日志：防共享接入日志、移动终端发现日志、准入日志、代理工具管理日志、登录/注销日志五个部分，其中防共享接入日志是用于查询内网用户通过代理、共享等方式上网的日志。

安全日志：包括上网安全和管理员操作日志，其中上网安全是开启上网安全服务后，记录上网安全行为的日志。

管理员点击[日志查询/所有行为日志]进行查询，可根据日期时间和过滤选项进行筛选。

管理员根据时间的时间和选项后，点击<查询>即可查到所有日志。



其他终端接入日志和上网日志的查询也跟所有日志查询一样操作。

用户行为分析

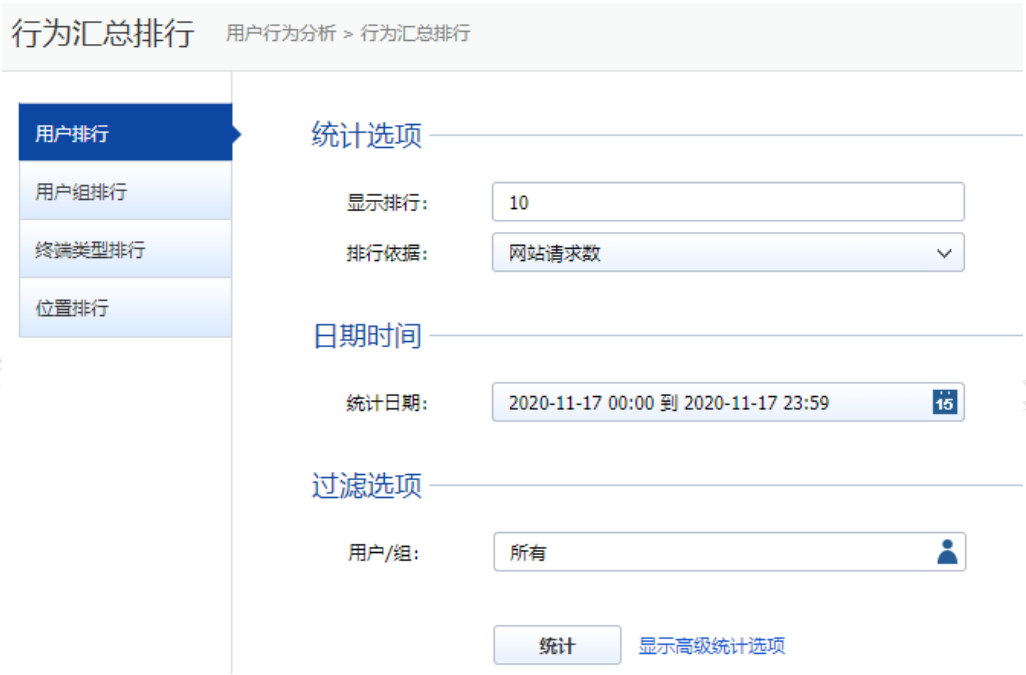
用户行为分析用于统计设备上网的用户行为次数。用户行为分析包括用户行为分析、网站分类分析、单用户分析三个部分。

用户行为分析：包括行为汇总排行、发帖/发微博排行、邮件收发排行、热门应用排行、文件审计排行、即时通讯排行、搜索关键字排行、应用行为趋势八个部分。

网站分类行为趋势：可以选择以用户（或用户组、终端类型、位置、网站分类）为统计对象，根据自定义统计选项、日期时间和过滤选项等信息进行趋势统计。

单用户分析：用于针对单独用户进行针对性的行为分析。

管理员可根据需要查询的流量通过选项统计、日期时间、过滤选项进行查询。



管理员选择完以后点击<统计>会生成结果如下所示。

流量时长分析

流量时长分析用于流量分析和时长分析，流量分析可统计应用流量排行、网站分类流量排行、域名流量排行、应用流速趋势、流控通道趋势、网站分类流速趋势；时长分析可统计应用时长排行、网站分类时长排行和域名时长排行。

- 流量时长分析用于流量分析用于统计通过设备上网的数据流量信息。
- 时长分析用于统计通过设备数据的时长信息。

其中应用流量排行查询以应用为对象，根据时间等信息进行流量统计并排行，包括用户排行、用户组排行、终端类型排行、位置排行、应用排行。管理员可根据需要查询的流量通过选项统计、日期时间、 过滤选项进行查询。

管理员选择完以后点击<统计>会生成结果如下所示。

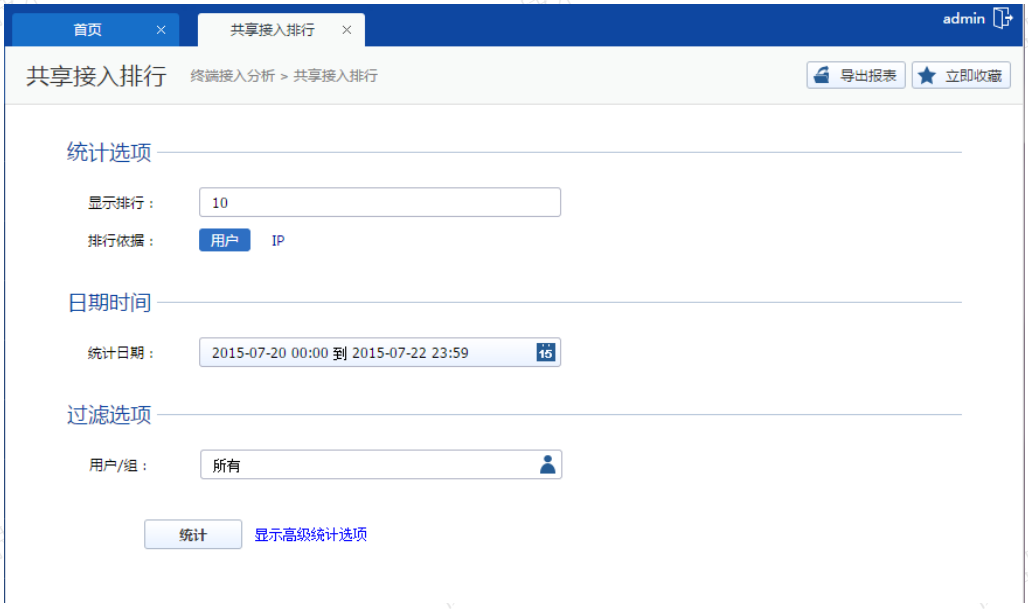
终端接入分析

终端接入分析包括共享接入排行、共享接入趋势、终端类型排行、终端发现趋势、用户活跃天数排行、接入用户数趋势和上网安全分析。

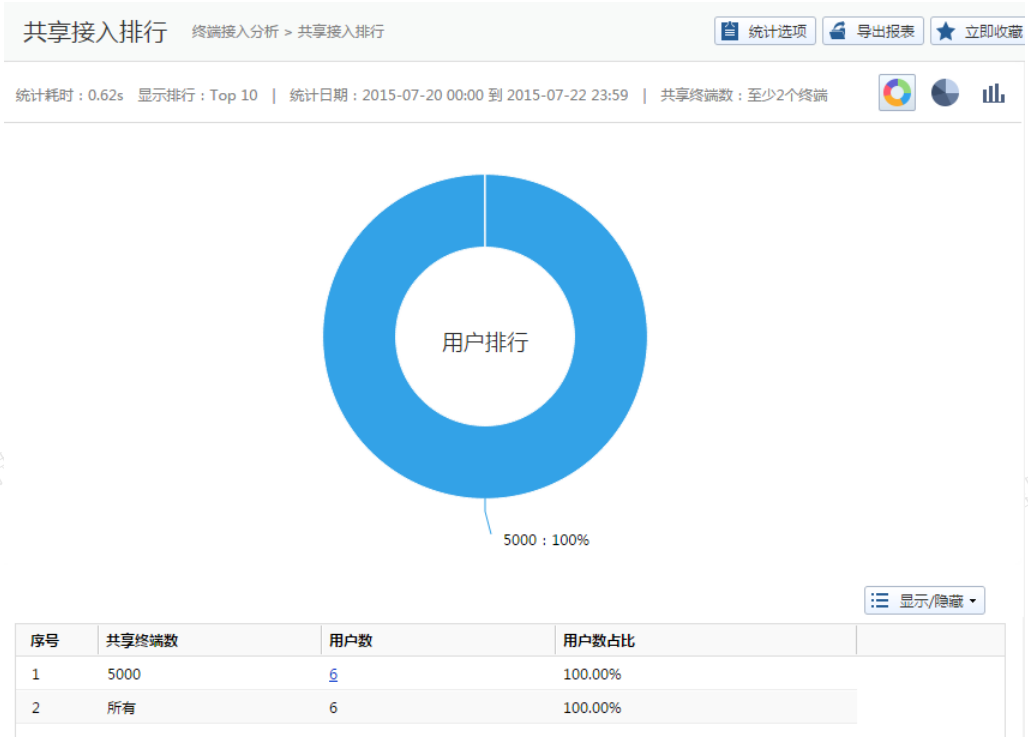
终端接入分析：用于检测终端接入到上网共享行为次数最多的用户和IP排行。

终端接入安全：用于统计上网安全事件的用户和事件类型。

管理员可根据统计选项、日期时间、过滤选项进行查询。



管理员选择完以后点击<统计>会生成结果如下所示。



业务分析

业务审计APP支持业务访问的查询功能，业务分析主要包括业务日志访问日志、服务器外联日志。

配置步骤

步骤1.管理员在[日志查询/业务访问日志]点击<查询条件>通过选项统计、日期时间、过滤选项进行查询。

步骤2.点击<业务日志查询>可以看到用户名称、业务名称、地址等信息。

步骤3.管理员点击<详情>能看到某条业务日志查询的详细日志信息。

带宽分析

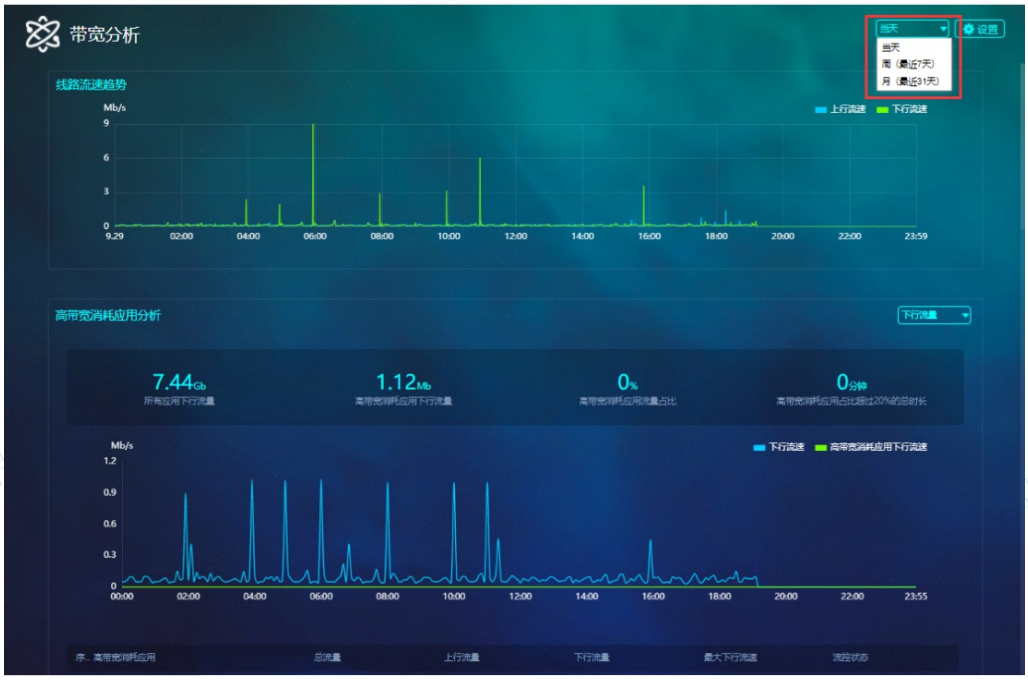
应用场景

当运维人员想了解内网带宽是否够用、高带宽消耗应用具体有什么，能从应用和用户维度了解流量的使用情况，从而能够及时对内网的带宽做一个调整分析，各个分支对接外置数据中心或日志分析平台成功后，在带宽分析应用针对单台设备进行分析。

配置步骤

步骤1.进入日志分析平台后选择[带宽分析]进入首页。

步骤2.在右上角选择查看的分支设备，可以查看当天、本周、本月的数据，在设备存在多条线路的情况下可以查看不同线路的带宽情况。



步骤3.点击<设置>跳转到超负荷和高带宽消耗应用配置页面，根据需要查询的应用进行分析，若是内置数据中心，则是没有分支设备选择；若是外置数据中心，则有线路的选择。

超负荷配置：设置超负荷判断条件，分别针对当天、周、月负荷设置条件。匹配条件则为超负荷。

高带宽消耗应用配置：设置高带宽消耗应用和自定义选择内网带宽消耗高的应用。

数据分析

根据设置后的条件，可以看到最近一天/周/月的带宽数据分析。可以根据带宽分析结果对分支某个应用流量比较大。

未关机检测分析

应用场景

随着发展企业办公电子化普及，提高了办公效率的同时，有些员工不良的工作习惯给企业造成了资源浪费，深信服提出具有绿色环保、节约企业资源的理念应用，通过对企业员工上网行为分析，识别出未关机的用户，为企业提供参考数据给企业节约资源。

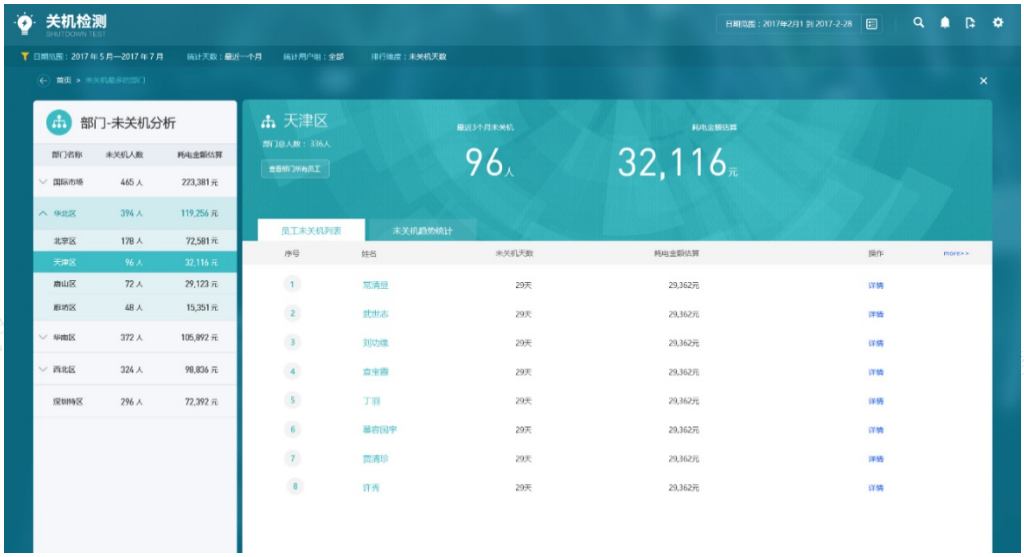
配置步骤

步骤1.进入日志分析平台后选择[未关机检测分析]，点击[立即配置]按钮设置对应组织结构。

步骤2.进入应用<设置>，根据实际需求设置未关机定义的耗电计算方法，当不需要设置未关机定义的员工可添加到白名单。

数据分析

设置了组织架构后可以查看未关机的人数详情和耗电估算。



没有符合条件的数据可能以下原因：

1. 请到系统配置页面检查是否配置同步策略并接入日志数据。
2. 请检查您是否开启用户流量审计功能（[行为审计/上网审计策略/流量与上网时长审计]）。
3. 如果以上都没问题，查询条件内暂时没有数据，您可以修改查询条件。

办公上网态势分析

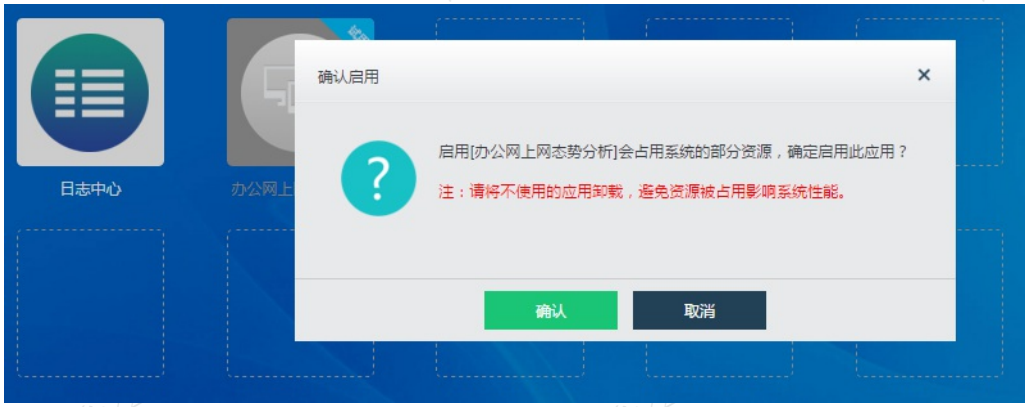
应用场景

适用于办公网的网络流量以及网络安全监控，通过收集全网行为管理的上网数据和下一代防火墙的安全数据，针对特定办公网提供网络管理和安全可视化，帮助管理员直观掌握整体网络上网概况，及时发现威胁并处理。

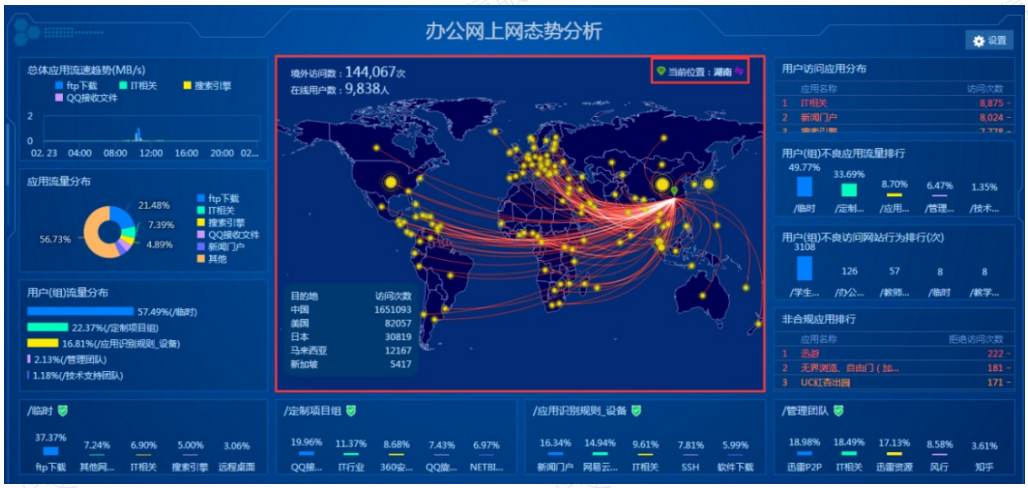
配置步骤

步骤1.进入[日志分析平台]后，点击[办公网上网态势分析]该图标后，弹出如下提示。

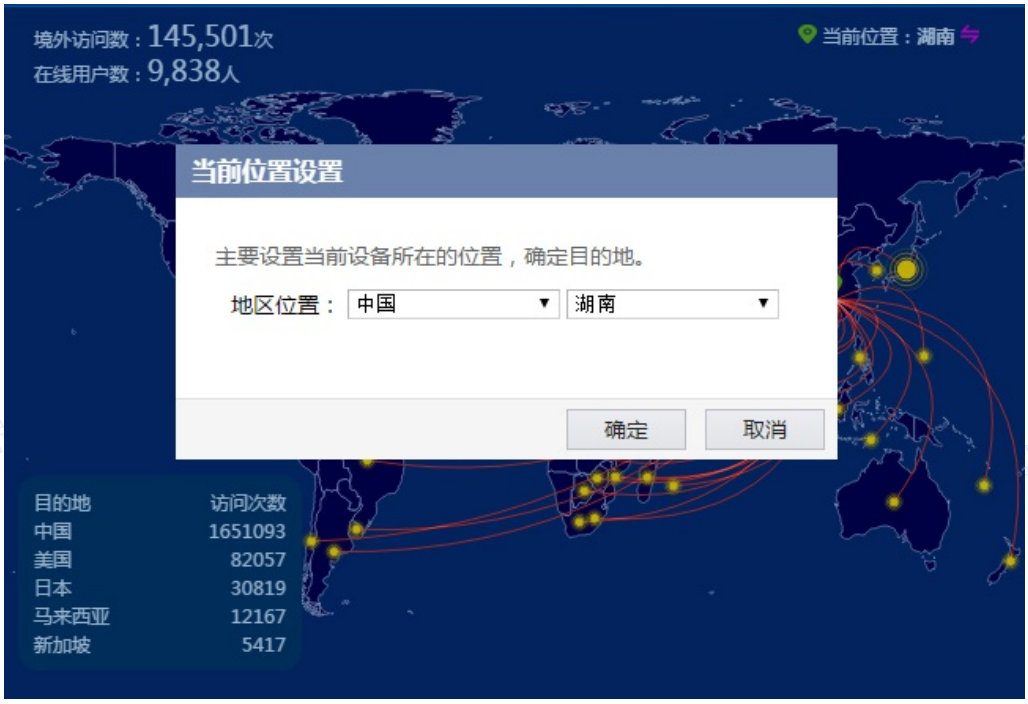
点击<新增>后启用该项功能。



步骤2.点击[办公网上网态势分析]图标后，直接进入[办公网上网态势分析]系统。



步骤3.如上图所示，在地图右上角点击<当前位置>，设置当前[地区位置]为您的所在区域，点击<确认>保存配置。地图中展示的是当前设备访问其他网络地址的情况。



步骤4.点击<设置>，进入办公网上网态势分析的配置页面，通过设置内容布局、不良内容定义、显示设置等3个部分内容，来定义展示内容。

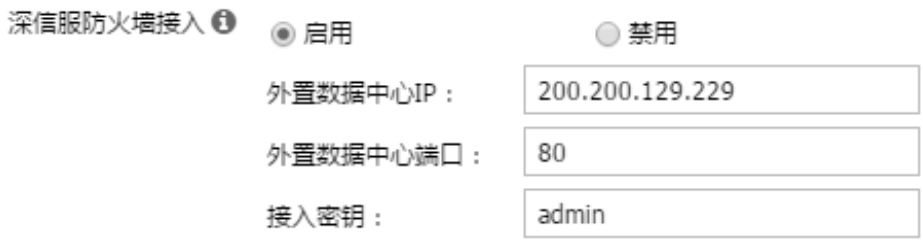
步骤5.点击<恢复默认配置>，可以将当前配置恢复为默认配置。

点击<保存>，可以将当前配置保存生效。

内容布局

[深信服防火墙接入]用于启用与深信服防火墙外置对接功能，启用后可以在展示屏上显示与防火墙相关的板块（需要您的防火墙外置数据中心支持对接）。

启用方法：点击<启用>，填写外置数据中心IP、外置数据中心端口、接入密钥即可。

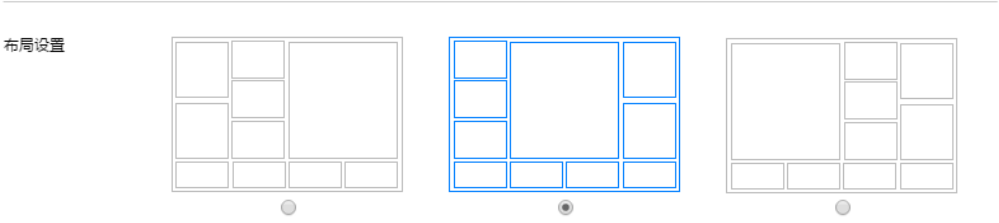


显示内容：分为[流量分析]和[安全分析]两个部分，勾选上的内容都会在首页上展示，选择的内容越多，展示的密度越大，择屏幕合适的分辨率进行展示。

流量分析：包含总体应用流速趋势、单位流量分布、热点单位轮播、应用流量分布、热门应用排行等5个内容。

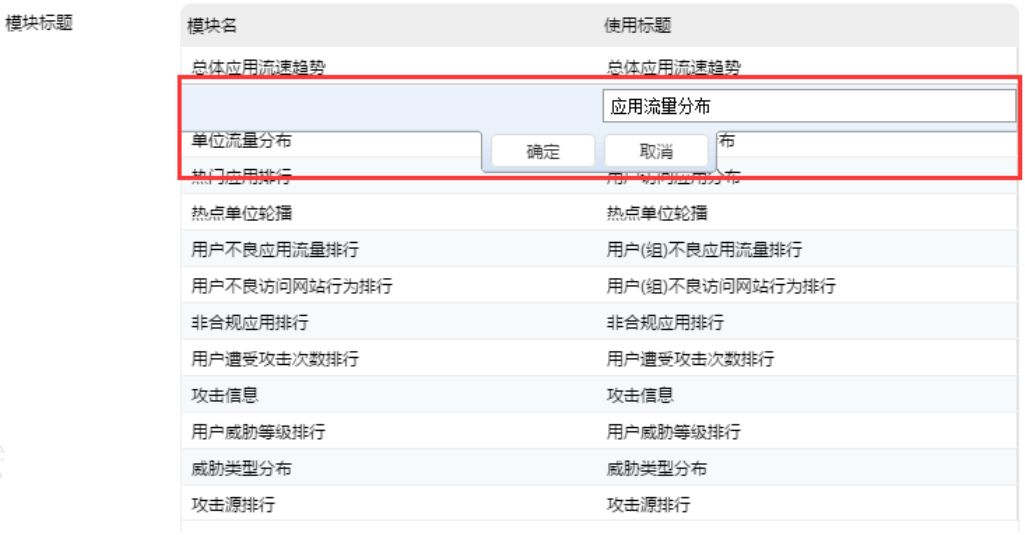
安全分析：包含用户不良应用流量排行、非合规性应用排行、攻击信息、威胁类型分布、用户不良访问网站行为排行、用户遭受攻击次数排行、用户威胁等级排行、攻击源排行等8个内容。

布局设置：根据需求调整整体布局模型，有大图居左、大图居中、大图局右3种选择。



标题设置：如下图所示，定义首页展示内容的大标题。

模块标题如上图所示，定义首页展示的各模块的标题名称。如下图所示，[模块名]为各模块名称，双击需要修改的模块所在行，即可编辑[使用标题]处的模块名称，修改完成后，点击<确定>保存配置。



不良内容定义

如上图所示，勾选首页需要展示的不良应用和不良网站。

不良应用定义：中勾选需要展示的具体不良应用类型。

不良网站定义：中勾选需要展示的不良网站类型。两者都支持模糊查询。

显示设置

查询维度：可选以用户组或用户为查询对象。

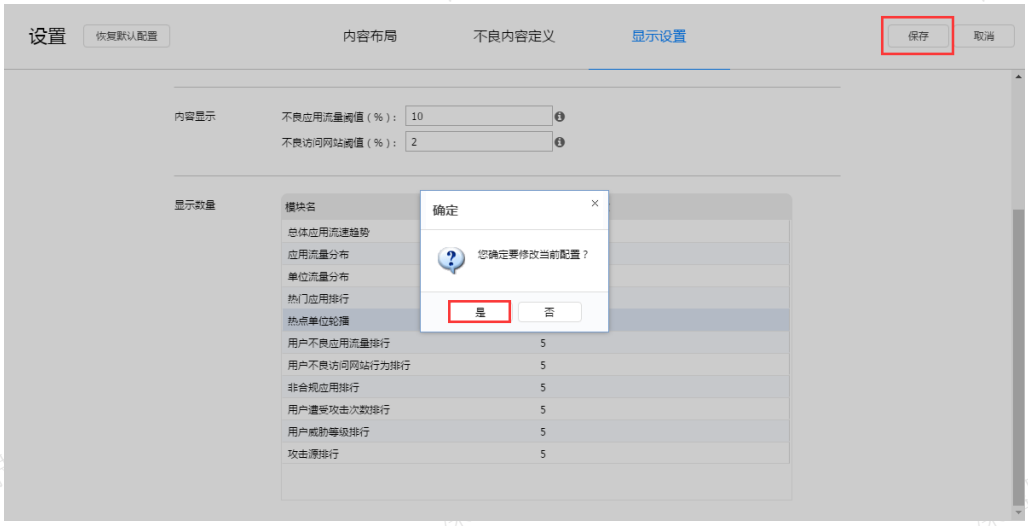
查询时间：定义查询当天最近多少小时的数据。

数据刷新频率：定义数据刷新的间隔时间。以秒为单位，默认为180秒，最小60秒，最大支持3600秒。

内容显示：定义不良应用流量阈值，即当不良应用流量占比超过所定义的阈值时，单位状态显示为异常。定义不良访问网站阈值，即当不良访问网站次数占比超过所定义的阈值时，单位状态显示为异常。

显示数量：定义首页展示的各模块的最大显示对象数。[模块名]为各模块名称，双击需要修改的模块所在行，即可编辑[最大显示对象数]，修改完成后，点击<确定>保存配置。注意：受展示框大小和美观度影响，请根据实际情况调整展示对象数量。

最后，点击<保存>，并点击<是>确认保存当前配置。



数据分析

如上图所示，鼠标移动到展示模块处，可以查询该模块展示内容的详细数据。

红框中展示的是[热点单位轮播]内容，会以滚动的方式展示每个热点单位的使用情况，默认以组为单位显示。如需修改为以用户为单位，则在[显示设置]中的[查询维度]处修改即可。修改后整个办公网上网态势分析都是以用户为单位的。

典型场景案例集

办公出口上网场景

需求背景

某公司租用了一条20Mb/s电信线路，内网有500名上网用户，为了保证内网安全方便管理员管理，员工需要通过AD域账号密码做身份认证后才能使用内网资源。而管理员在上班时间段发现很多市场部人员经常使用P2P下载工具进行下载，占用了大部分带宽，影响了其他部门的正常的办公业务，公司希望通过将市场部的这部分数据占用的带宽限制在2Mbps之内。同时根据公司业务需求，要保证财务部门访问网上银行网站和收发邮件的数据，在线路繁忙时所拥有的带宽不能小于2Mbps，但最大不能超过5Mbps。为了保证内部知识产权的安全，公司禁止员工在内网环境下访问微博以及其他论坛等应用，同时还需要审计员工访问互联网内容。

需求分析

根据该公司的上网需求，可以在AC上开启Portal认证功能，在用户入网前结合企业AD域来做Portal认证核实接入网络员工的身份信息。为了限制市场部人员的P2P下载流量，可以通过AC流量管理模块的流控策略对这部分数据做限制，同时也可以通过流控策略保障公司财务部的带宽资源。通过AC的访问权限策略，禁止员工在内网环境下通过微博和论坛发帖，最后再通过SSL解密策略识别员工访问互联网内容。

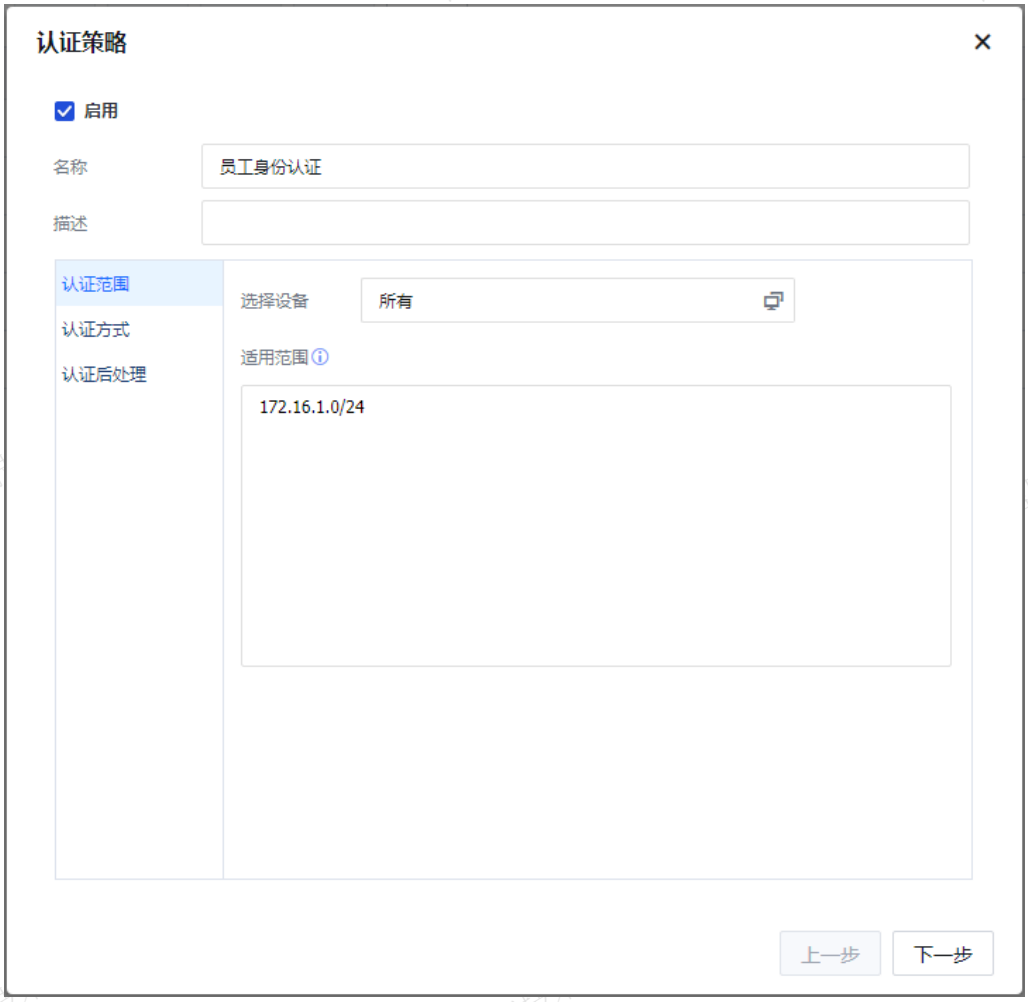
配置步骤

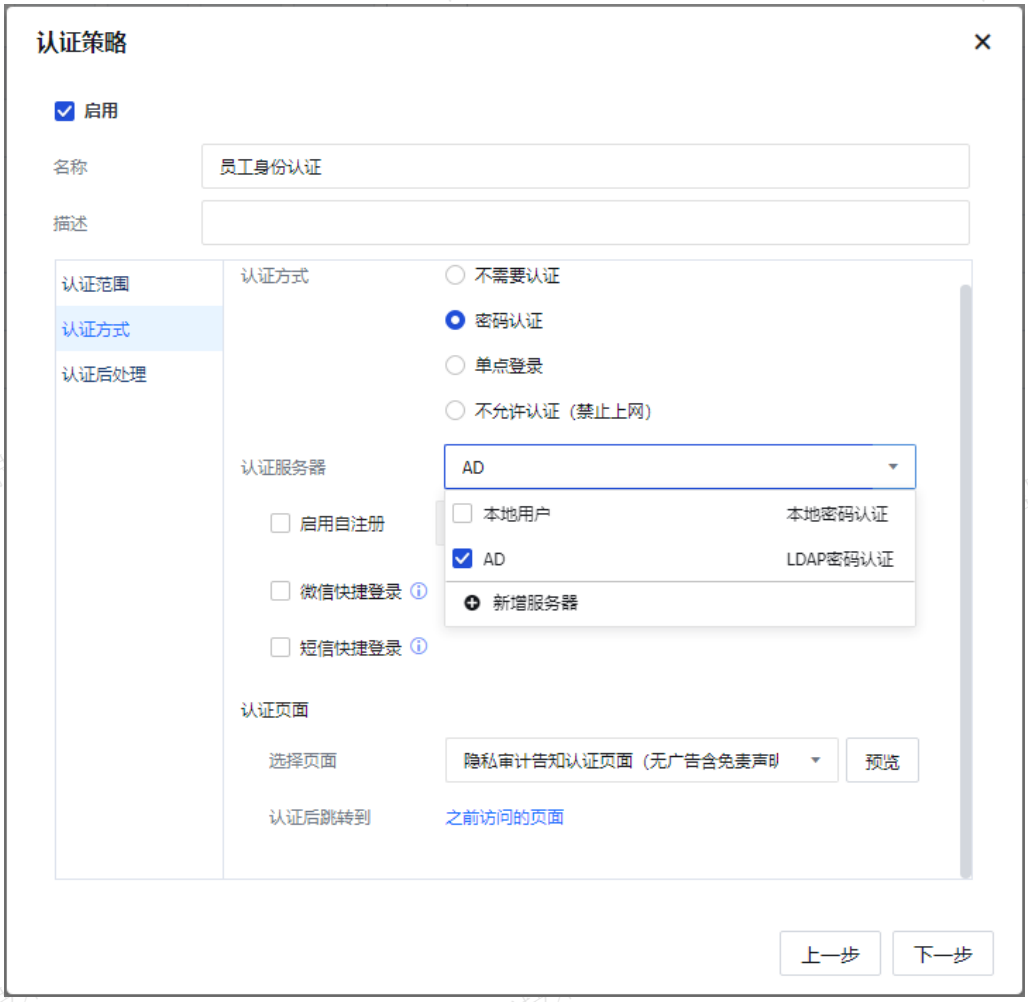
步骤1.为了获取员工AD域身份信息，需要先在AC的[接入管理/接入认证/Portal认证/认证服务器]对接公司的AD域服务器。

步骤2.在认证服务器点击<新增>按钮，选择[LDAP服务器]对接公司的AD域服务器。在对接时需确认公司的AD域服务器是否开启了加密传输，如果有请勾选[加密选项]并导入相关证书，最后再测试有效性。（本示例中域名为ac.com,请参考修改相关信息）。

步骤3.在AC的[接入管理/接入认证/Portal认证/认证策略]栏点击<新增>按钮，配置Portal认证策略。

步骤4.在认证策略点击<新增>按钮，在弹出的[认证策略]框中填写策略名，在[认证范围]的适用范围填写内网用户网段，在[认证方式]中选择“密码认证”并在认证服务器栏内勾选对接好的公司AD域。最后点击<提交>即可。





步骤5.配置流控策略，限制市场部P2P下载流量，在AC的[流量管理/虚拟线路配置]页面点击<新增>按钮，配置一条与公司出口线路带宽一致的虚拟线，用于对应出口线路。

⚠ 注意 ：

虚拟网线配置在网桥模式才会默认显示这个节点，路由模式要开启虚拟线路模式才显示。

步骤6.在AC的[流量管理/流控策略]页面点击<新增通道/新增一级通道>按钮，添加一条流量一级通道。在[新增一级通道]的配置界面填写好[通道名称]，在[带宽通道设置]栏中的[生效线路]栏选择前文新建的对应出口线路的虚拟线路名，勾选[限制通道]并按照公司要求填写相应的带宽值，因为是限制P2P下载的流量最后需要勾选[抑制P2P下载丢包]。

步骤7.在[新增一级通道]的配置界面选择[通道使用范围]栏。在[适用应用]栏选择自定义再勾选所有的P2P应用，在[适用对象]栏选择自定义勾选好市场部人员。最后点击<确定>提交策略。

步骤8.在AC的[流量管理/流控策略]页面点击<新增通道/新增一级通道>按钮，添加一条流量一级通道。在[新增一级通道]的配置界面填写好[通道名称]，在[带宽通道设置]栏中的[生效线路]选择对应出口线路的虚拟线路名，勾选[保证通道]并按照公司要求填写相应的带宽值。

步骤9.在[新增一级通道]的配置界面选择[通道使用范围]栏。在[适用应用]栏选择自定义再勾选邮件和网上银行应用，在[适用对象]选择自定义勾选好财务部部人员。最后点击<确定>提交策略即可。

步骤10.配置访问权限策略和SSL解密策略。在AC的[行为管理/访问权限策略]页面点击<新增/访问权限策略>按钮，添加一条访问权限策略。在[访问权限策略]的配置界面填写好[策略名称]，勾选[策略设置]栏的[应用控制]，点击<应用控制>界面的<新增>按钮，在弹出的[选择适用应用]界面勾选微博以及论坛的全部内容。

步骤11.然后点击[适用对象]栏勾选所有用户，最后点击右下角的<提交>保存。

步骤12.在AC的[行为管理/SSL解密策略页面点击<新增/SSL解密策略>按钮，添加一条SSL策略。

步骤13.在[SSL解密策略]的配置界面填写好策略名称，在解密方式栏依据用户的实际环境选择中间人机密或者客户端代理解密。

⚠ 注意 ：

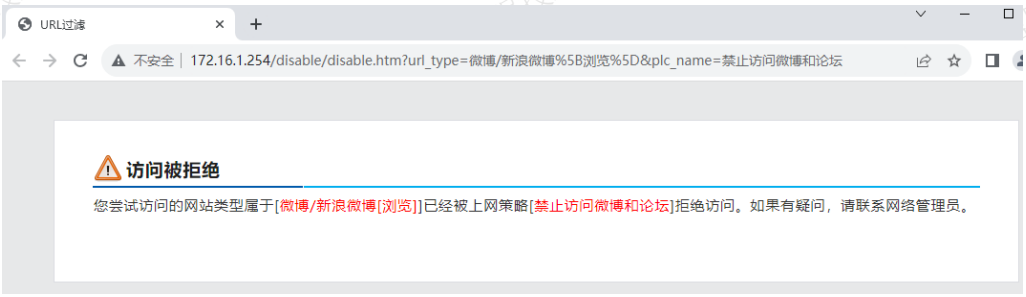
证书无效浏览器告警的话需要在浏览器导入根证书。通常使用场景是通过域统一推送。

效果预览

1. Portal认证未通过认证前。

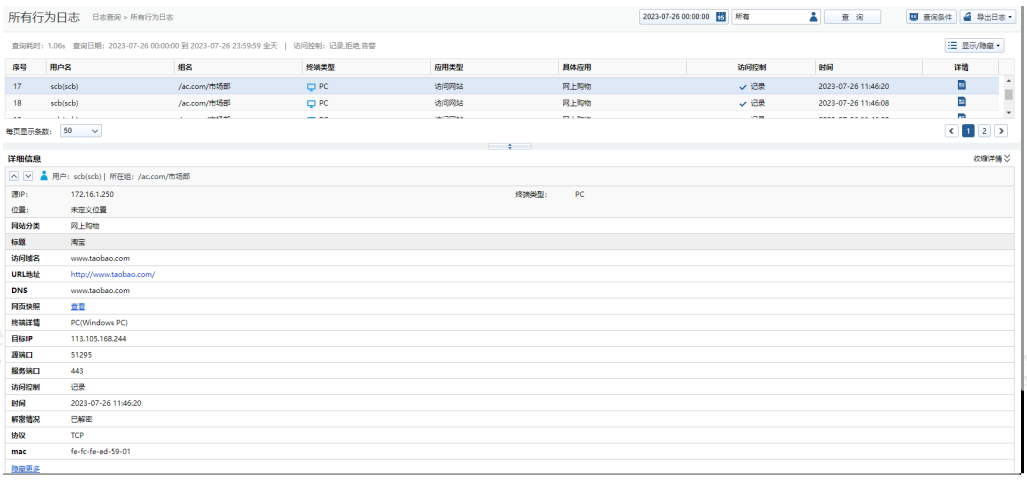
2. 使用域账号通过认证后。

3. 禁止访问微博和其他论坛。



4. 在[全网监控/上网行为监控]查看员工上网行为审计。

5. 在[日志中心]查看员工上网行为日志。

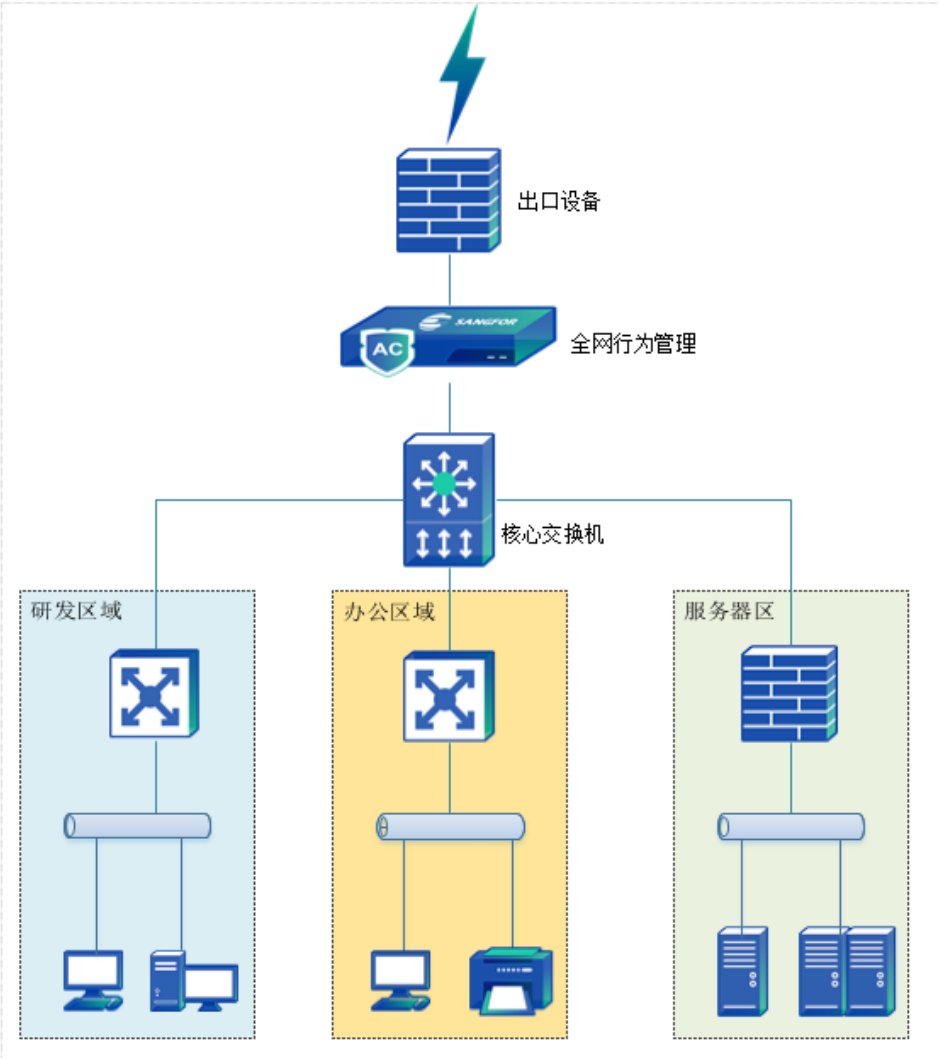


终端准入管控场景

需求背景

某互联网公司内存在大量终端设备，这些终端设备没有经过可信认证就随意接入内部网络，给内网安全带来了极大的安全隐患，如携带病毒接入导致病毒蔓延等威胁。同时，这些终端接入网络后访问权限缺乏管控，给业务系统带来极大的威胁。该用户需要一种既能做到可信接入内网，又能对终端进行有效管理，确保不可信、不合规的终端不能接入网络。其中，为了防止研发部门泄露公司源码，需要禁止非法访问外网和禁止接

入U盘等存储设备。用户的网络拓扑如下图所示。



需求分析

针对该用户的需求进行解读，可通过以下几个功能点来进行具体实现。

1. 802.1X认证：对终端上网用户做强管控，未通过认证不能访问内网服务器资源和外网资源，满足可信接入的需求。哑终端设备免认证上网。
2. 杀软检查：要求终端上网用户必须安装公司要求的杀毒软件。
3. 非法外联检查：禁止研发部门PC非法访问外网行为。
4. U盘管控：禁止研发部门接入U盘设备。

配置步骤

步骤1.配置802.1X认证。

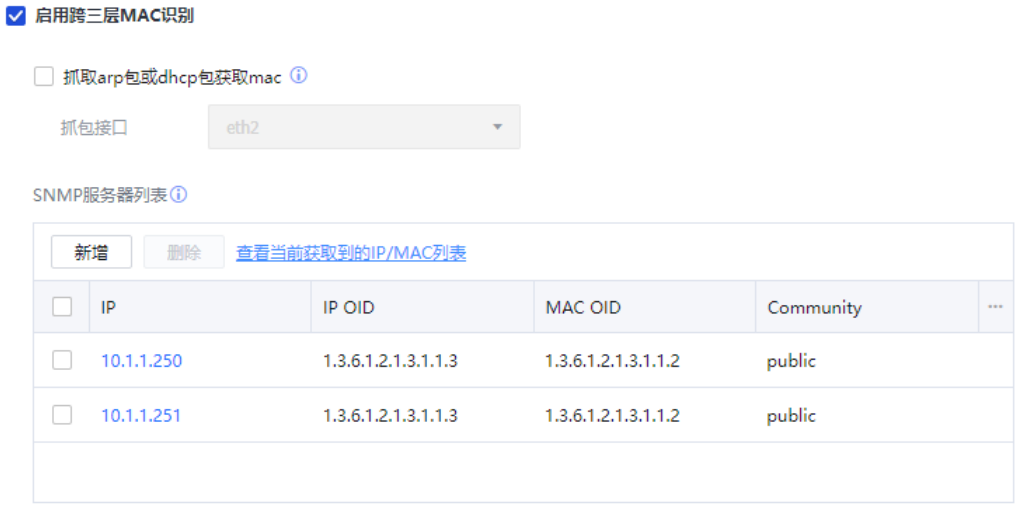
进入[接入管理/接入认证/802.1x接入认证]，勾选启用按钮开始配置。在[认证方式]启用本地密码认证。

步骤2.选择本地密码后，在[接入管理/用户管理/本地组/用户]栏添加本地用户。

步骤3.接入交换机802.1x配置

对应交换机启用802.1x功能，认证服务器选择radius，radius服务器指向AC，交换机配置请参考《交换机802.1x配置工具V2.0》。链接地址：https://bbs.sangfor.com.cn路径：自助服务/常用工具/交换机802.1x配置工具。

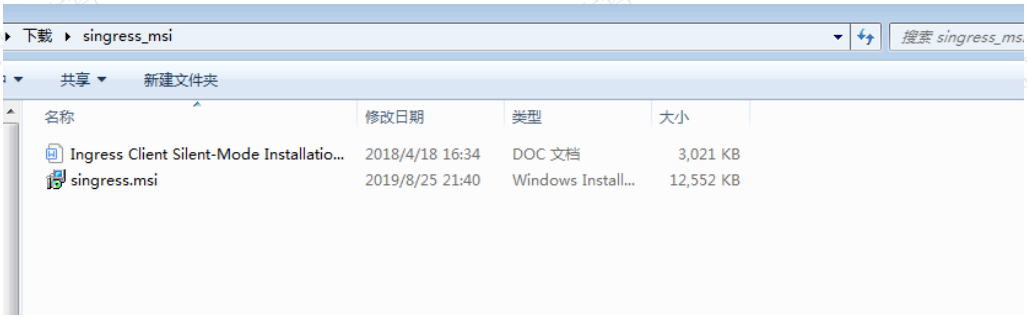
步骤4.通过SNMP获取终端MAC地址。配置SNMP服务器，需要交换机开启相关服务，在[接入管理/接入认证/联动对接设置/跨三层取MAC]，启用跨三层取MAC识别，新增SNMP服务器（交换机）。



步骤5.认证助手配置，在[接入管理/终端管理/准入客户端配置]中勾选[开启准入认证客户端的802.1X功能]并设置准入客户端网关地址。

步骤6.点击[点击下载准入MSI安装包]下载准入插件安装包，或者通过终端PC访问互联网AC重定向准入客户端的安装页面来进行下载，也可手动访问（http://ACIP/sinstall/sinstall.htm）。

步骤7.下载解压之后以管理员权限安装singress.msi，注意勾选开启准入认证客户端802.1x功能才会生成快捷方式。



步骤3.安装完成之后会在桌面生成快捷方式。

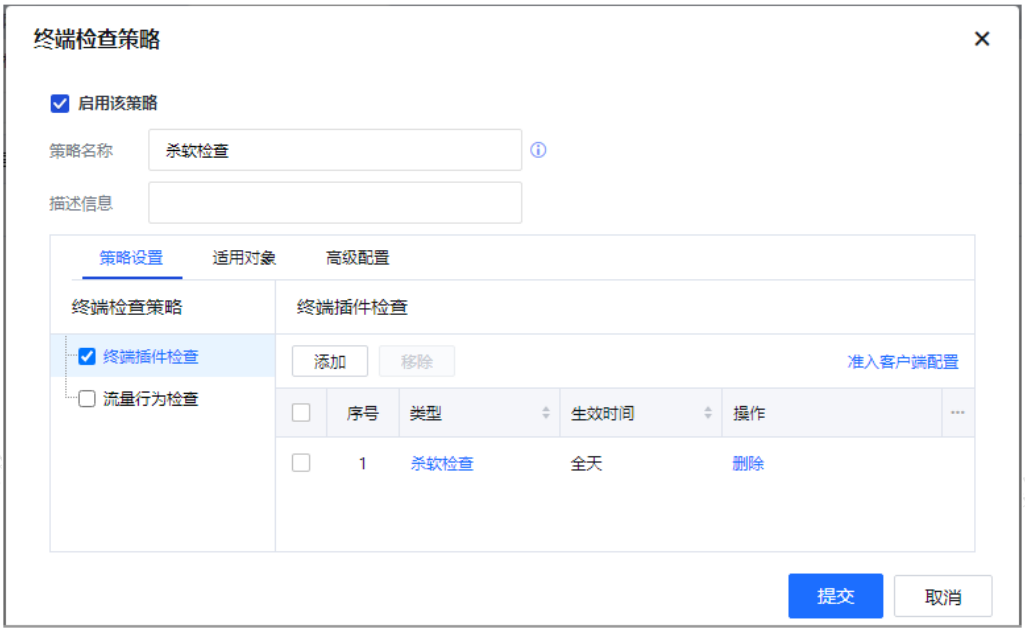
步骤8.用认证助手时注意右上角选择正确的网卡。

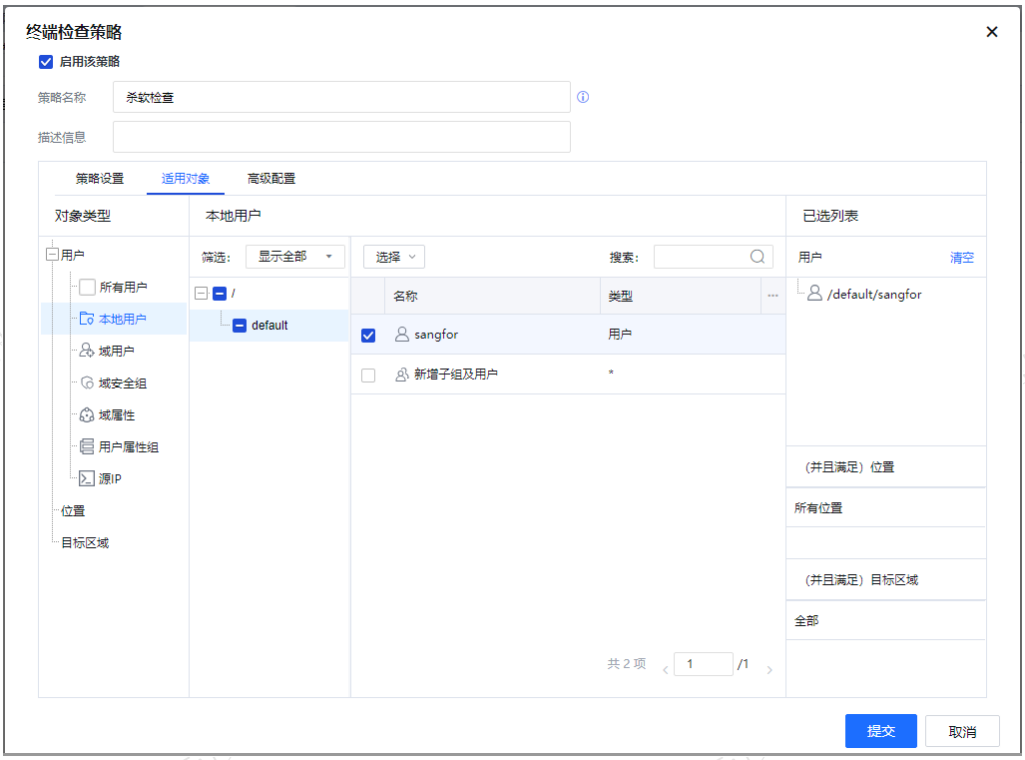
步骤9.配置杀软检查。

在导航菜单中的[接入管理/终端管理/终端检查规则/插件检查规则]，然后点击<新增>，然后选择查<杀软检查规则>。

步骤10.在杀软检查规则中填入规则名称、规则类型、规则描述，勾选EDR终端防护，同时设置检测病毒库未更新的天数为30天，超过30天病毒库未更新则认为是违规。

步骤11.在[接入管理/终端管理/终端检查策略]中新建终端检查策略，引用“杀软检查规则”，同时选择适用用户。

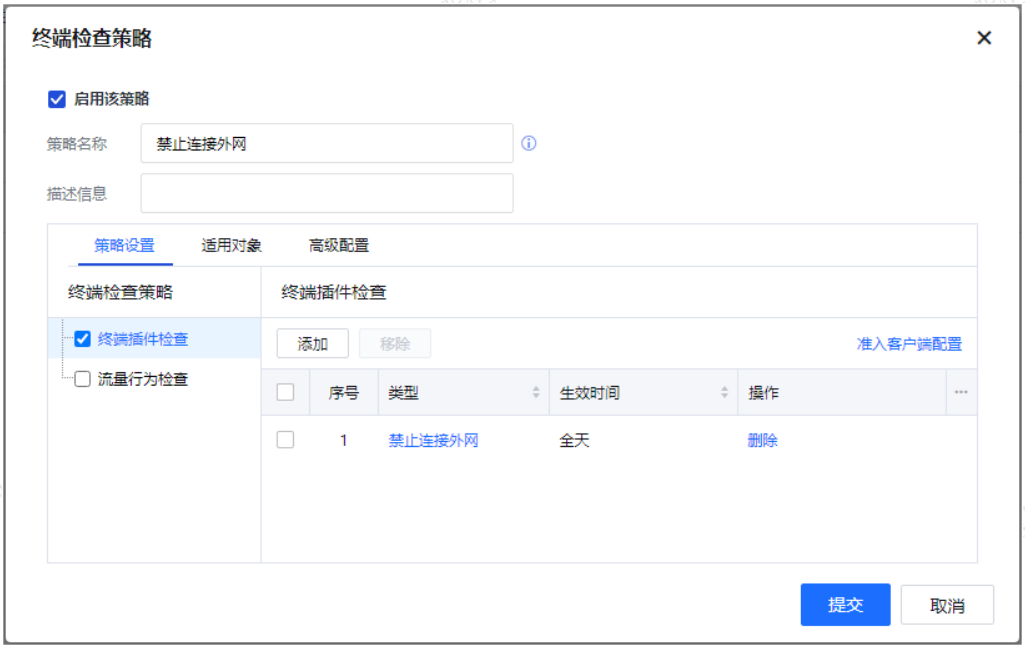


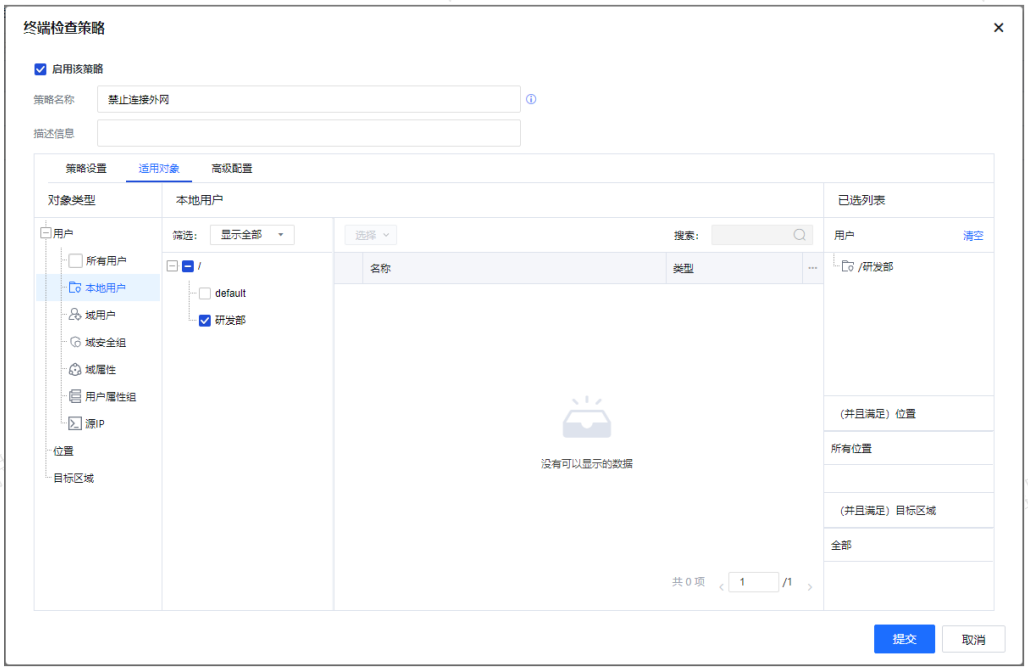


步骤12.配置非法外联检查。

在导航菜单中的[接入管理/终端管理/终端检查规则/插件检查规则]，然后点击<新增>外联检查规则。填写好规则名称，规则类型、规则描述，并在[检查项配置]勾选<连接外网>。在违规设置处设置[违规处理]为断网。

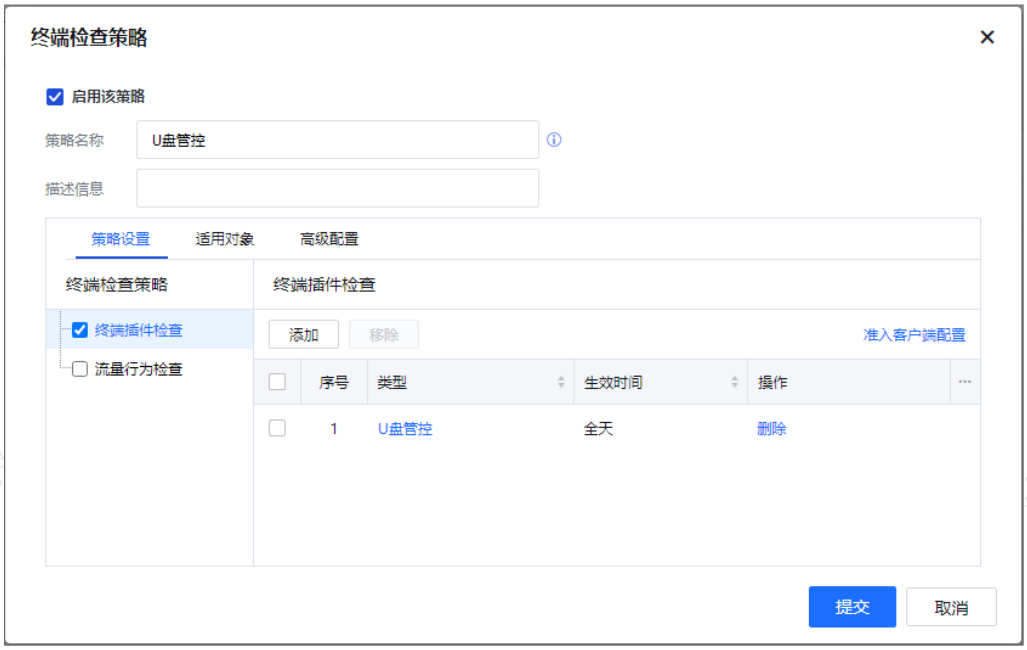
步骤13.新增检查策略，引用<禁止连接外网>规则类型，选择适用对象为研发部门。





步骤14.配置U盘管控。

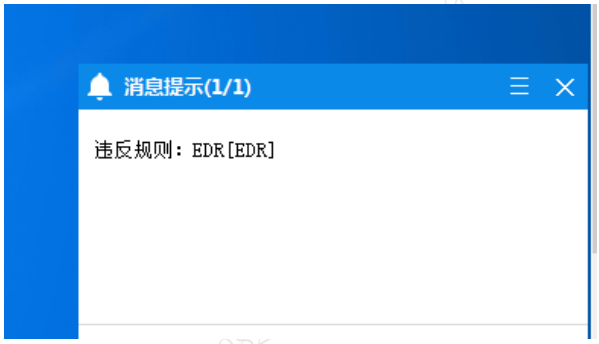
在导航菜单中[接入管理/终端管理/终端检查规则/插件检查规则]，设置规则名称和规则类型，勾选需要禁止使用的外设类型为存储设备。然后在检查策略中关联适用对象。

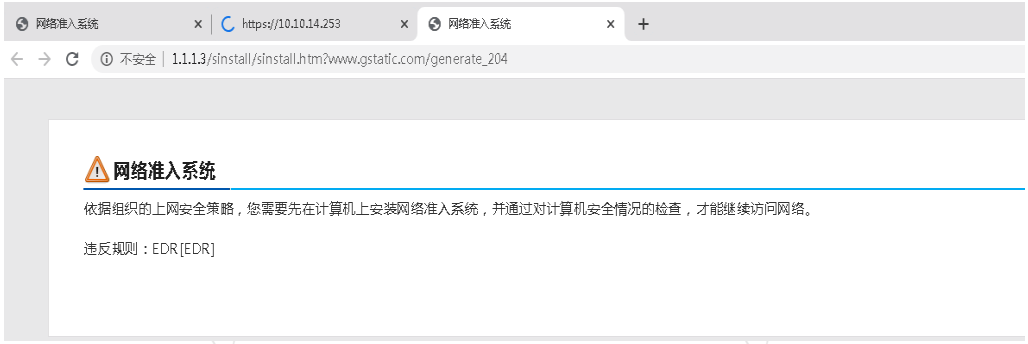


效果展示

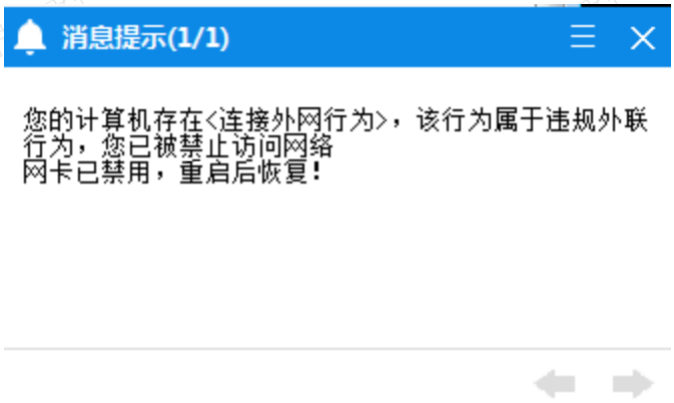
1. 802.1X本地密码认证成功。

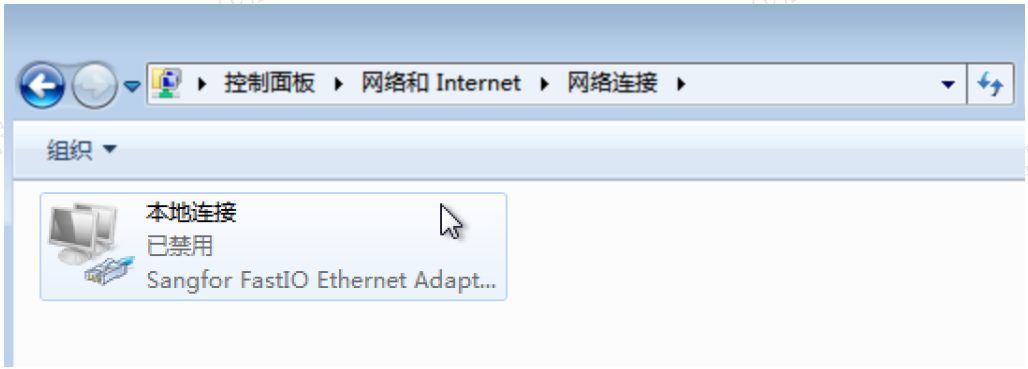
2. 杀软检查未安装EDR终端的终端无法上网并被要求安装EDR软件。



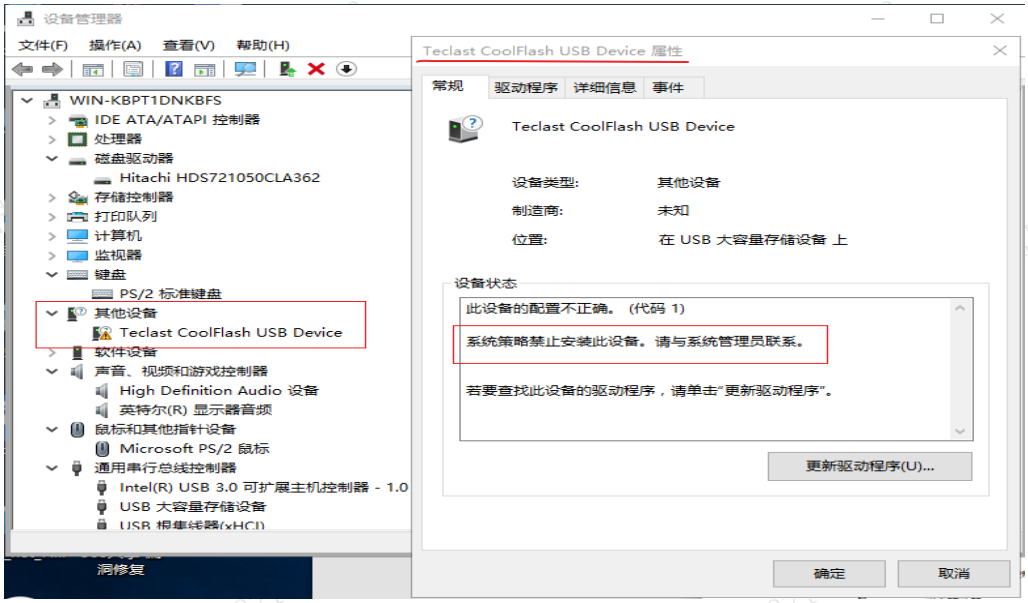


3. 非法外联检查研发部门终端连接外网时无法访问网络，并且网卡被禁用。





4. U盘管控研发部门终端插入违规U盘等存储设备显示未被加载。



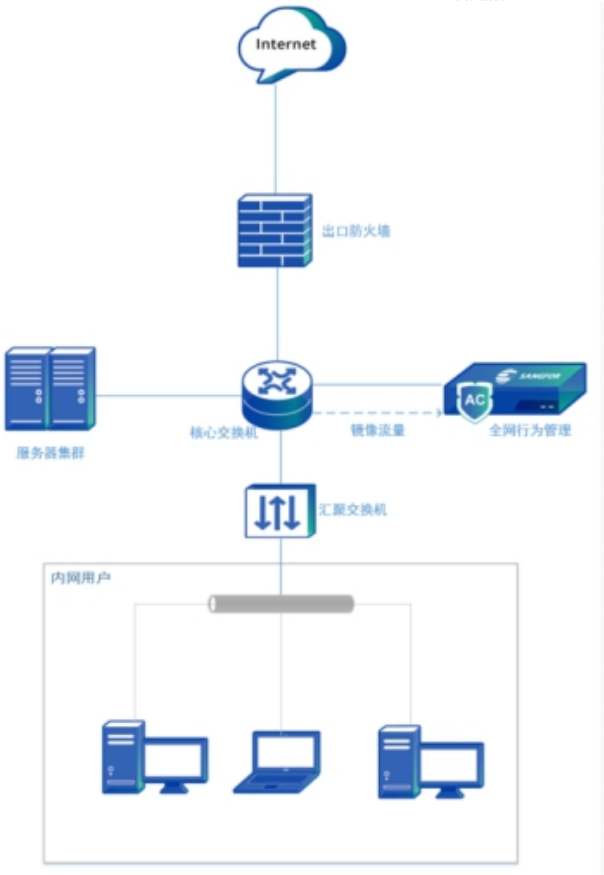
外发审计场景

需求背景

用户为国内知名医疗器械设计生产公司，为了防止商业机密泄露和自主知识产权外泄，需要审计内部员工使用QQ和微信外发文件、U盘拷贝文件、网盘上传、邮件外发、以及通过浏览器外发的文件，同时还要审计内部员工从内部服务器上拷贝的文件内容。

需求分析

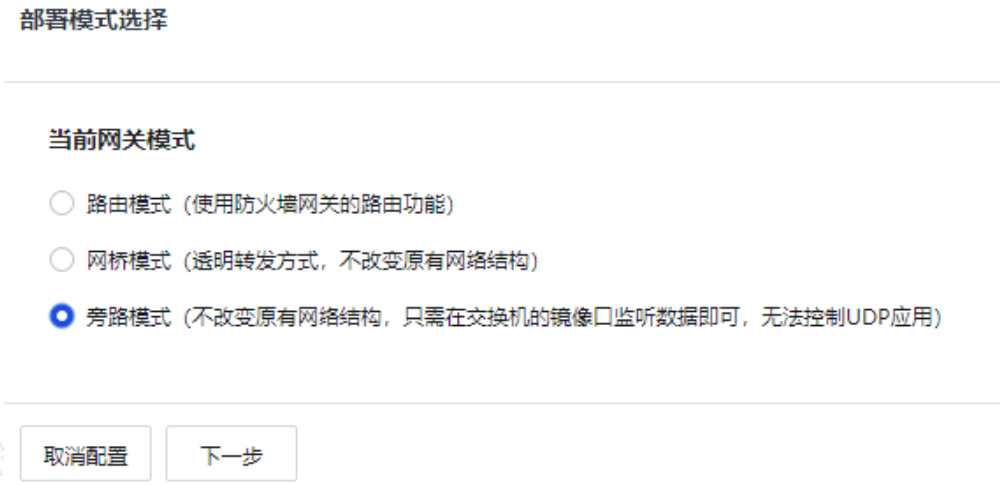
针对用户的该需求，通过部署深信服AC设备，并在内网用户使用的终端上安装准入客户端即可实现。同时为了最小化部署AC设备的工作量，可以将AC设备旁路部署在用户内网流量的汇聚点。（如下图所示）在用户核心交换机上既可采集到内网用户外发的流量，又能够采集到访问服务器集群的流量。因此将AC设备旁挂到用户核心交换机，并将核心交换机上的流量镜像给AC设备。



配置步骤

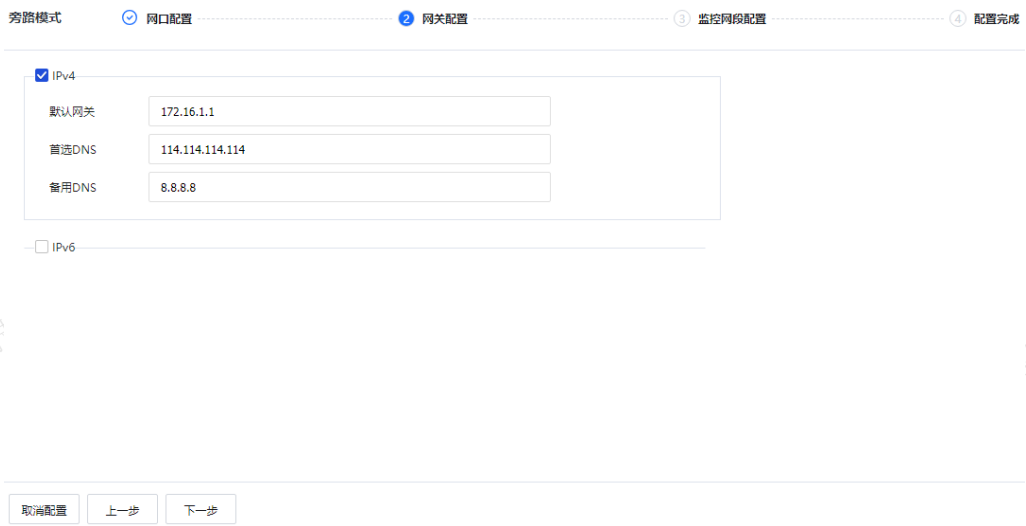
第一步：以旁路模式部署深信服AC设备。

步骤1.在导航菜单栏进入到[系统管理/网络配置/部署模式]栏，选择旁路部署模式开始配置。

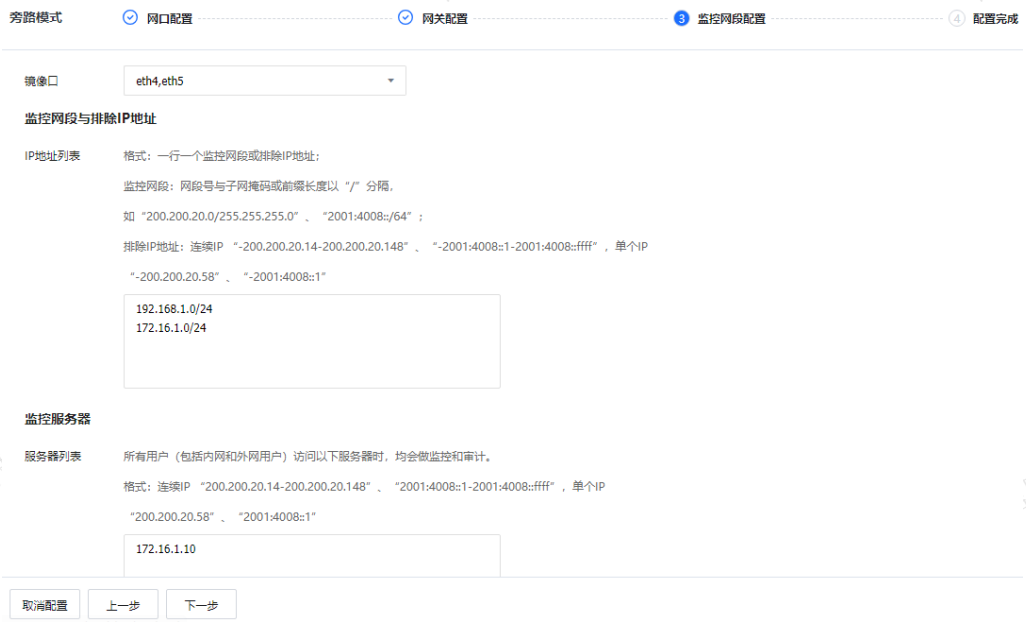


步骤2.选择管理接口并配置对应的IP地址，管理IP需要能够与安装准入客户端的PC通信。

步骤3.配置管理口默认网关和DNS。



步骤4.配置镜像口、监控网段以及服务器地址。当用户内网存在多份镜像流量需要AC审计时，可以在AC上配置多个镜像口用于接收不同源的镜像流量。



步骤5.确认配置无误后，点击完成重启设备。

第二步：配置交换机镜像流量。（本次以H3C交换机配置示例）。

<Sysname> system-view

#进入配置模式

[Sysname] mirroring-group 1 local

#创建名为“1”的本地镜像组

[Sysname] mirroring-group 1 mirroring-port G/0/1-G/0/8 both

#将交换机G0/0/1-G0/0/8口作为镜像源端口添加到镜像组“1”中，源端口可以按照用户实际情况来选择。必须将源端口的inbound和outbound双向流量均镜像给AC设备，示例命令中的both参数即表示镜像源端口的双向流量。

[Sysname] mirroring-group 1 monitor-port G0/0/9

#定义镜像流量的目的端口为G0/0/9口。

通过上述示例命令，将交换机G0/0/1-G0/0/8的双向流量均镜像到交换机的G0/0/9口，此时在交换机的G0/0/9口即可监听到G0/0/1-G0/0/8口所有的会话，最后将交换机的G0/0/9口与AC的镜像口连通。

⚠ 注意：

1. 源端口的总流量大小不能超过目的端口的带宽大小，否则会丢失部分数据包，造成审计不完整的现象。同理，从交换机镜像到AC设备的镜像流量大小不能超过AC设备镜像口的带宽。

2. 源端口必须镜像双向的流量，即inbound和outbound的流量，否则无法正常审计。

3. 需要审计的业务的流量必须镜像到AC，否则无法审计。

第三步：推送并安装准入客户端。

可以通过AD域策略推送准入助手，也可以借助用户内部第三方桌管平台推送安装。或者重定向到准入助手的下载界面，让用户自行下载安装。

⚠ 注意：

客户端审计需要借助准入助手来实现，与802.1x认证的准入助手为同一个软件。在不开启准入功能时，准入

助手安装后默认隐藏。

第四步：配置审计策略

步骤1.配置SSL解密策略，因为涉及到审计邮件外发以及审计网盘上传等场景，需要先配置好SSL解密策略。

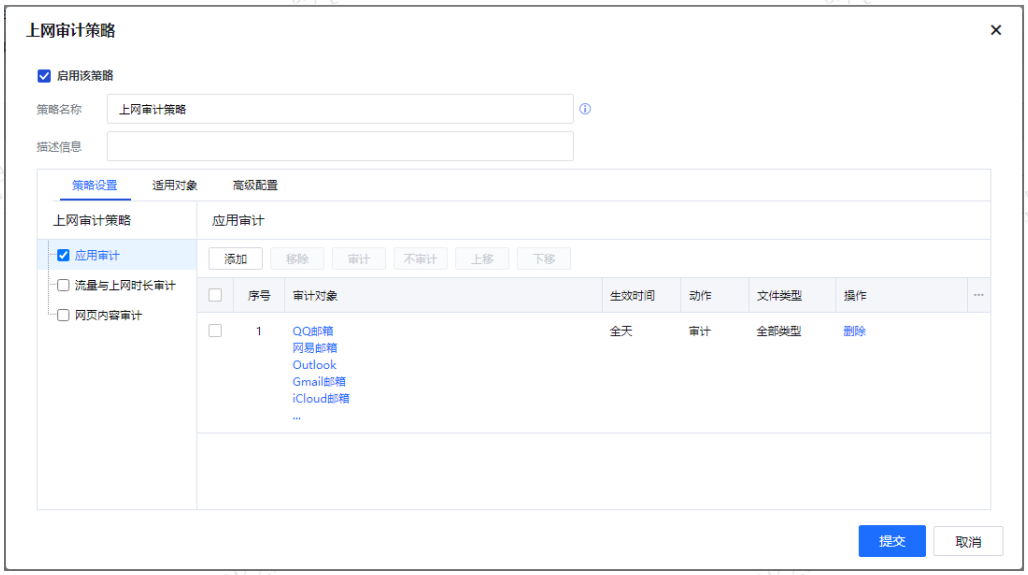
步骤2.在导航菜单栏的[行为管理/SSL解密策略]栏，点击<新增>添加SSL解密策略。

在配置页面[界面方式]选择客户端代理解密，降低解密对设备性能的损耗。

步骤3.勾选[加密WEB应用内容识别]以及[加密邮件内容识别]，仅识别使用25、465、995、143、993、587端口的SMTP加密邮件内容。

步骤4.配置上网审计策略，为了能够审计网页版的邮箱外发以及网盘上传，在[行为审计/上网审计策略]中点击<新增>按钮，添加相应的上网审计策略。

步骤5.勾选[应用审计]，在右侧的配置栏中点击<添加>按钮，勾选Web邮箱、网盘、HTTP外发与下载等审计对象，在配置好适用对象后点击<提交>即可。

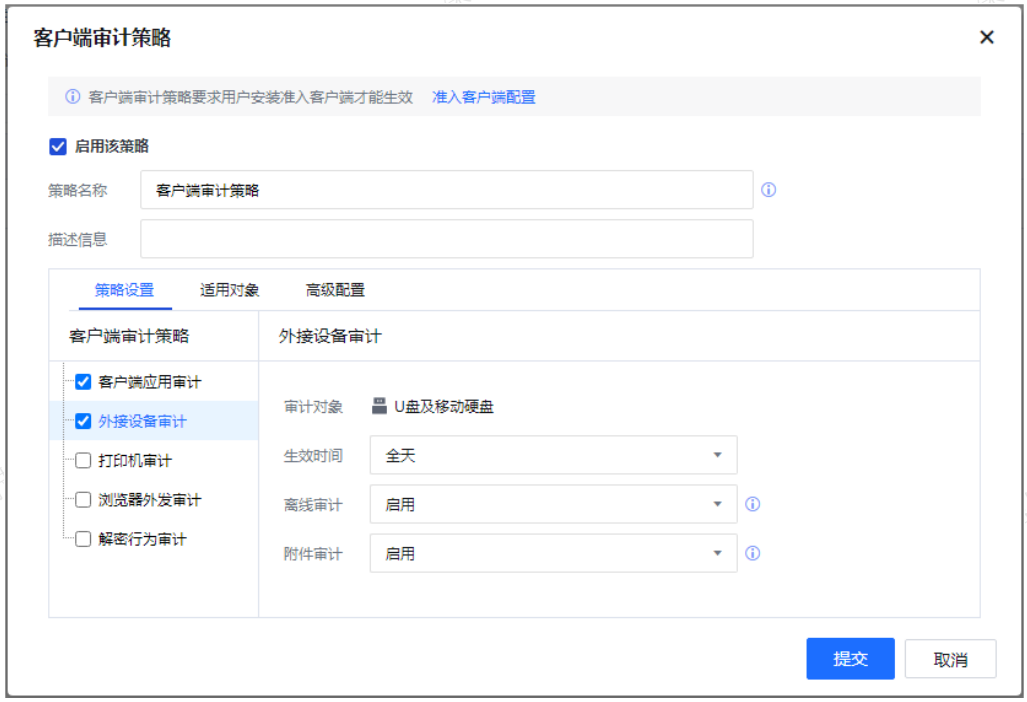


步骤6.配置客户端应用审计策略

在[行为审计/客户端审计策略]栏中点击<新增>按钮,选择客户端审计策略。勾选[客户端应用审计]策略，并在右侧的配置栏中勾选邮件客户端等审计对象，在配置栏底端的[离线审计]选择启用，最后配置好适用对象后点击提交即可。

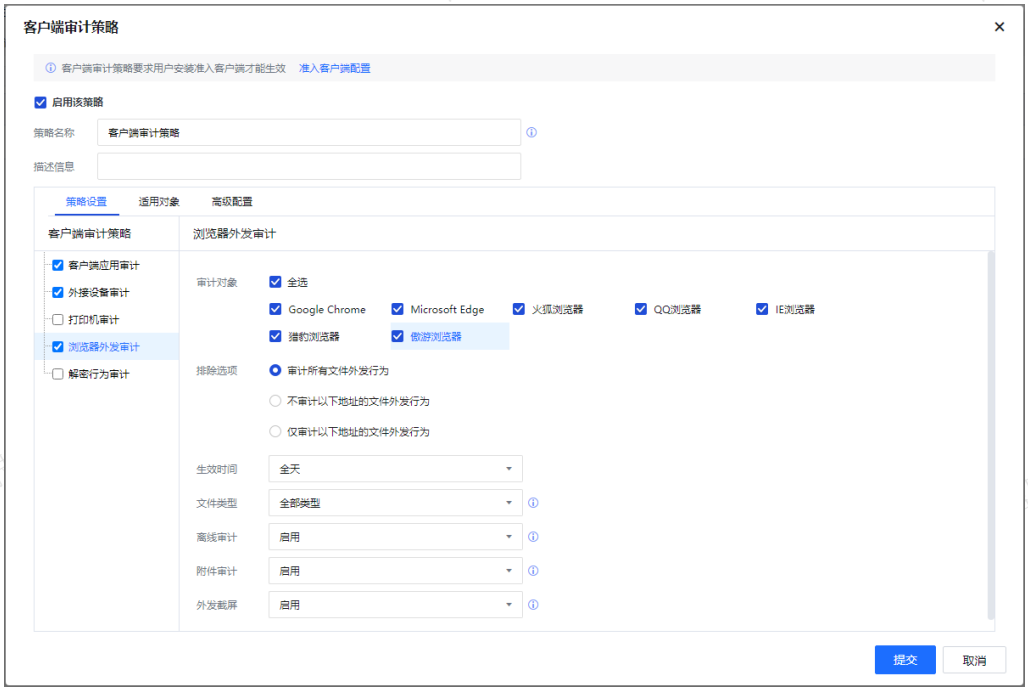
步骤7.配置U盘审计策略

在[行为审计/客户端审计策略]栏中点击<新增>按钮,选择客户端审计策略。勾选[外接设备审计]策略后，在配置栏勾选[移动存储介质]选项，如果需要可以勾选[离线终端审计]功能。在配置好适用对象后点击提交保存即可。



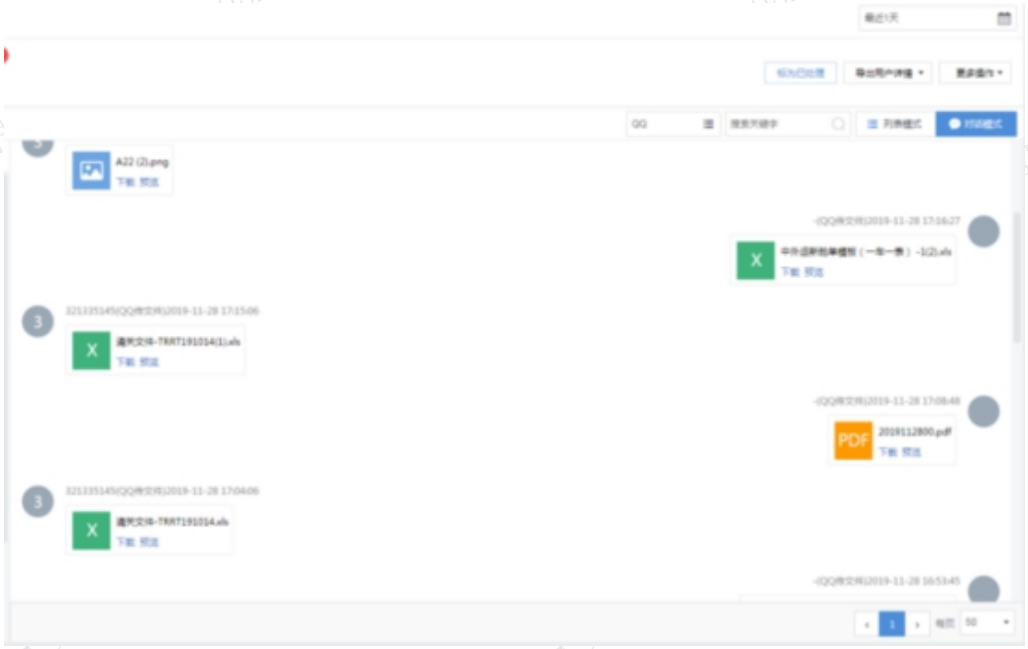
步骤8.配置浏览器外发审计策略。

在[行为审计/客户端审计策略]栏中点击<新增>按钮,选择客户端审计策略，勾选[浏览器外发审计]，选择需要审计的浏览器。

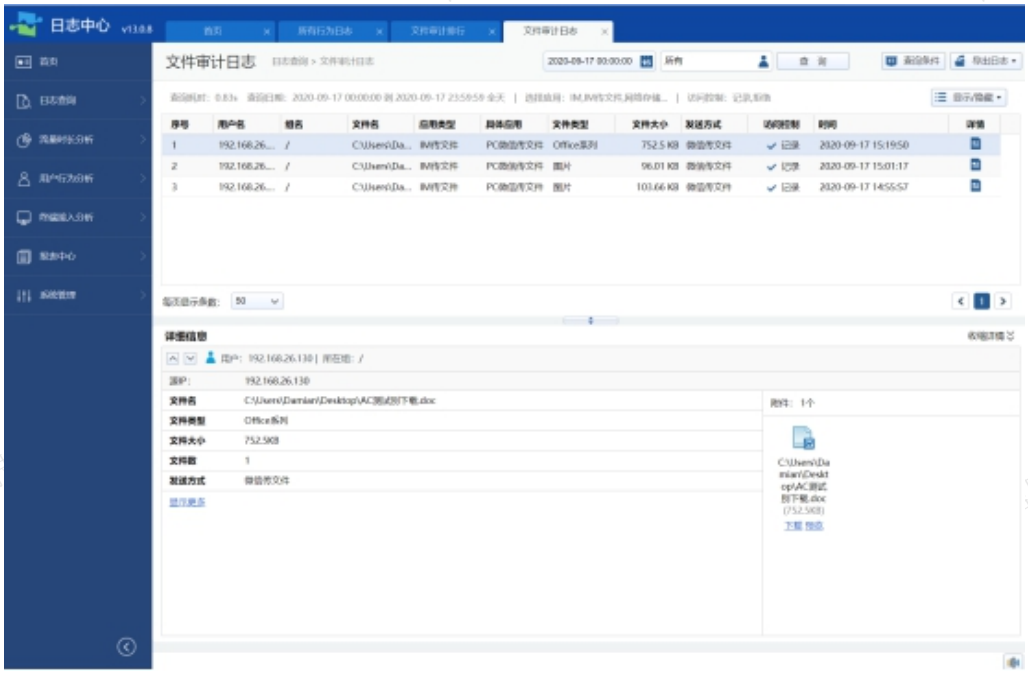


效果预览

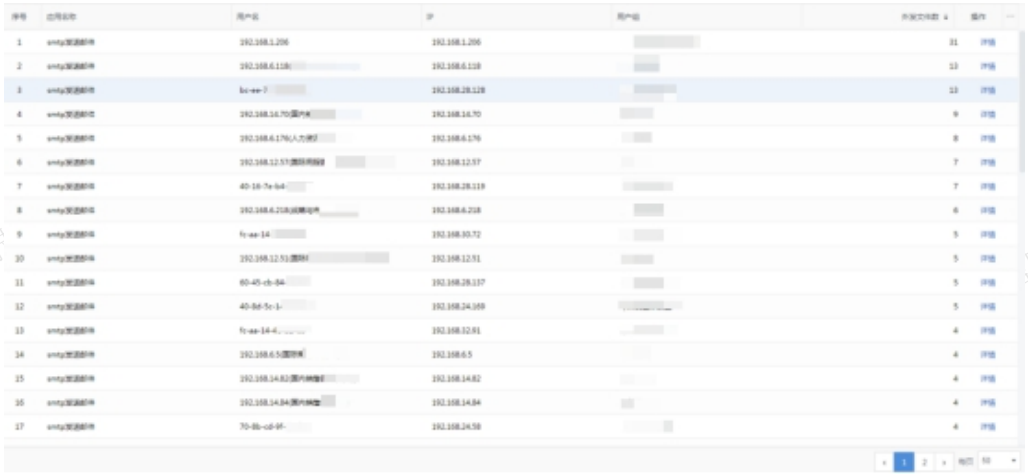
1. QQ外发文件审计结果。

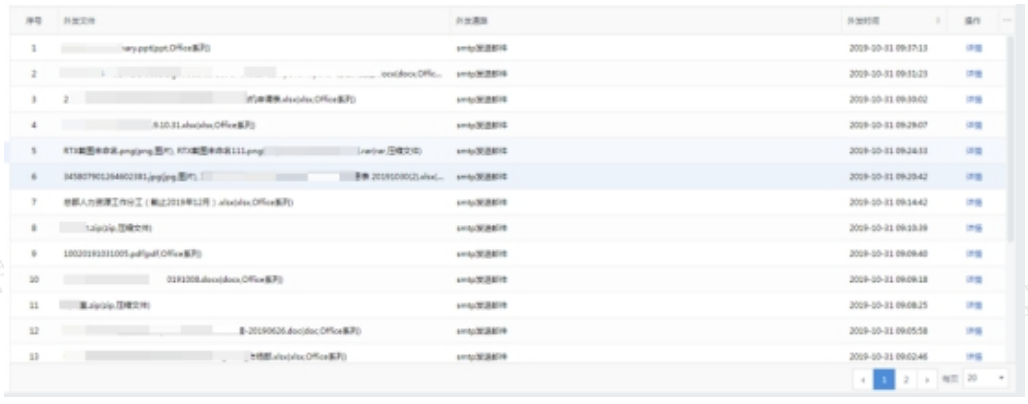


2. 微信外发文件审计结果。



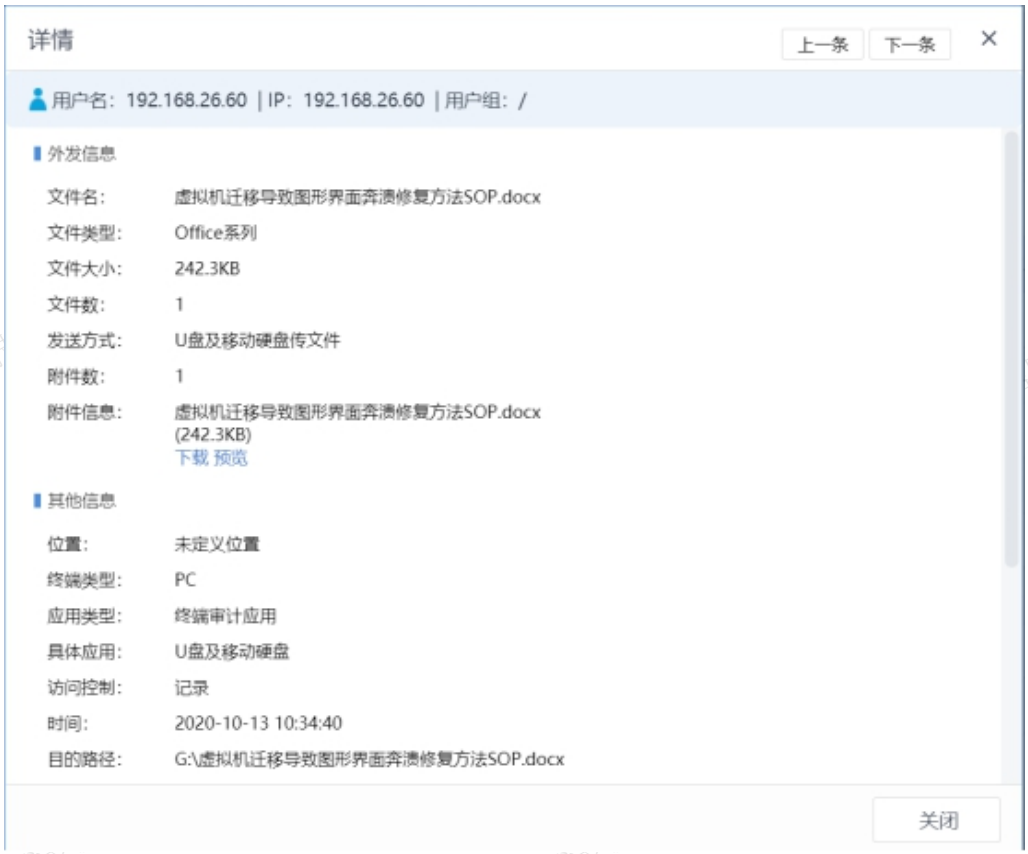
3. 邮件外发文件审计结果。



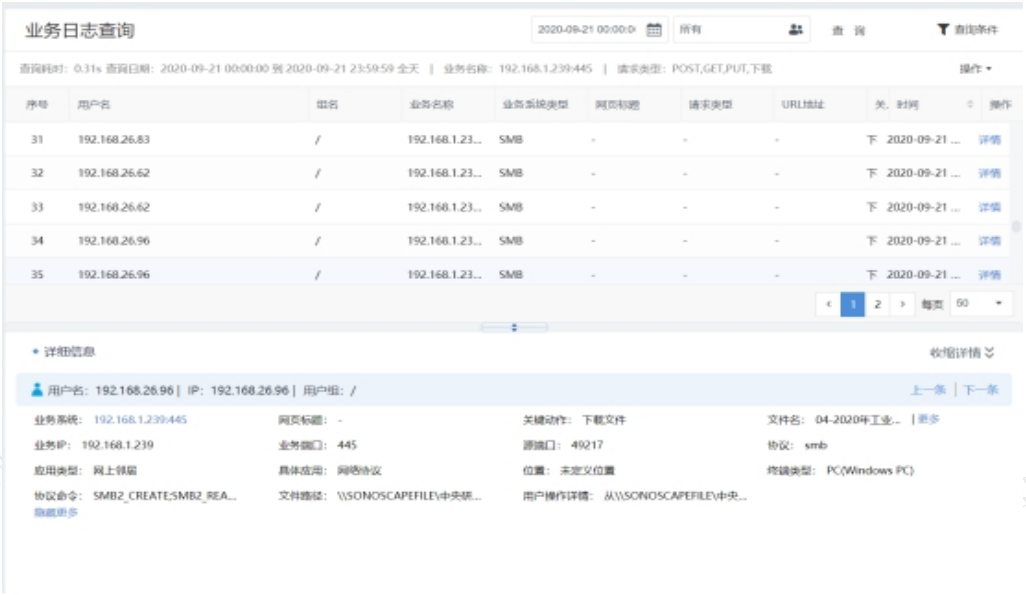


4. 网盘外发文件审计结果。

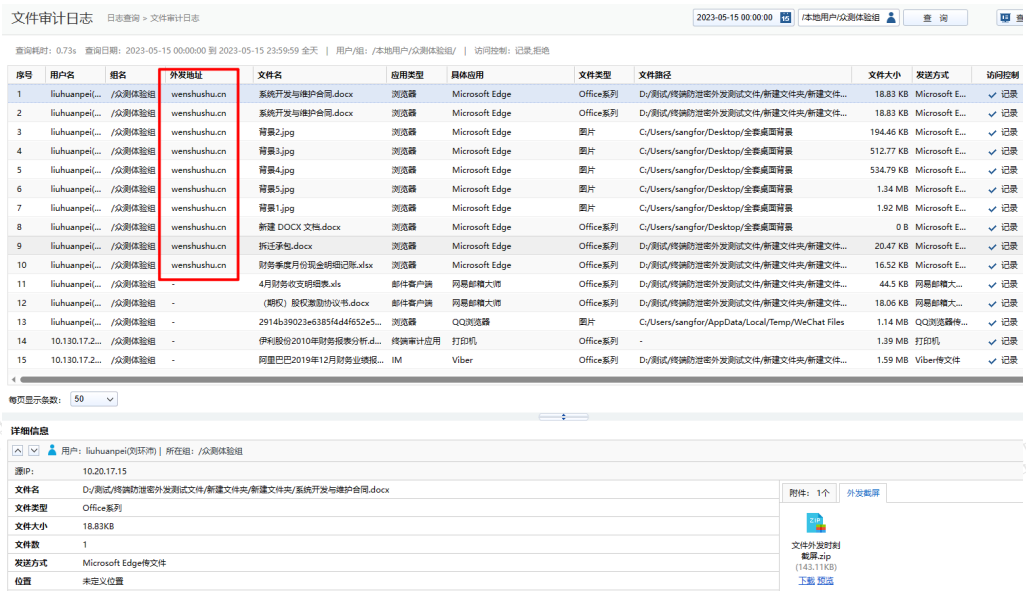
5. U盘拷贝文件结果。



6. 通过SMB协议从业务服务器拷贝文件。



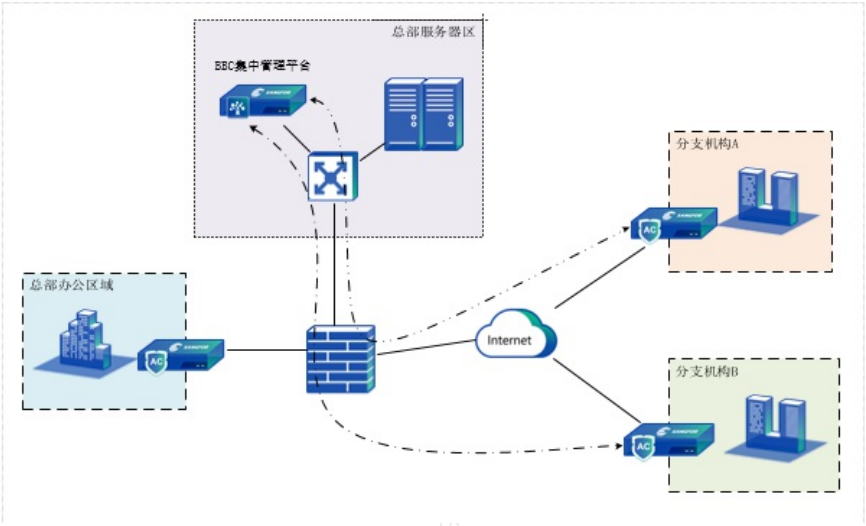
7. 通过浏览器外发文件，可以在“上网行为监控”和“日志中心”中查看。



多分支组网场景

需求背景

某房地产公司有多个分支机构，每个分支均设有深信服的AC设备，总部已购置了一台深信服BBC集中管理设备，现需要通过集中管理平台实现总部对分支的统一认证、统一管控和统一审计。用户侧网络拓扑图如下所示。



需求分析

针对该用户的需求进行解读，可通过以下几个功能点来进行具体实现。

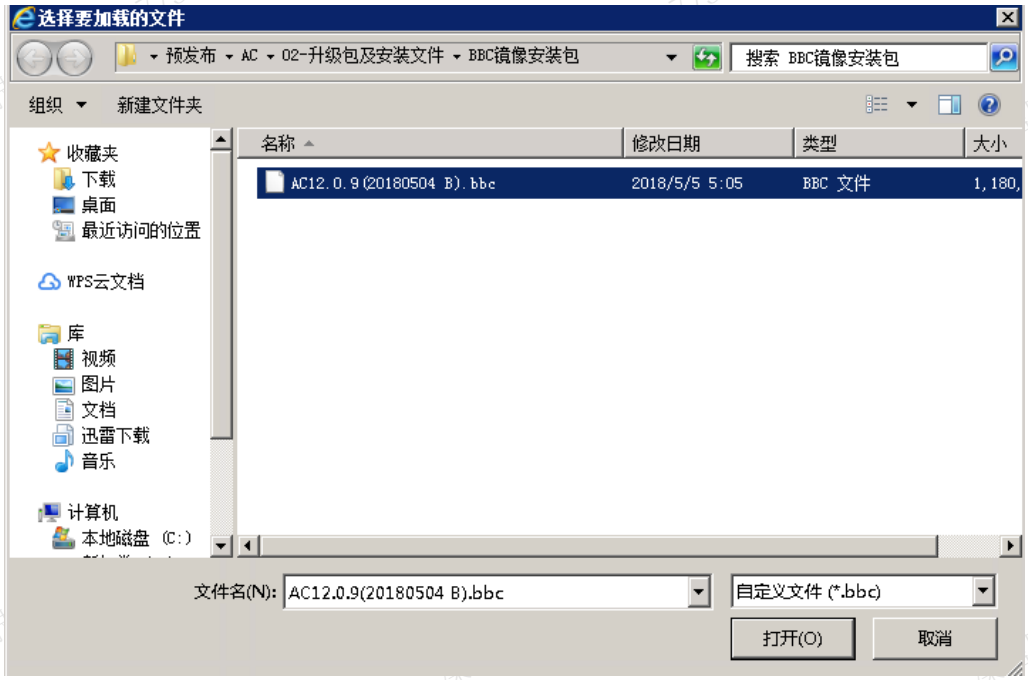
1. 统一认证：BBC对接AC认证中心，分支AC对接BBC，BBC给分支AC下发认证托管策略。认证中心上配置认证策略，分支AC的用户通过认证中心AC进行认证，实现用户认证统一在认证中心AC维护。
2. 统一管控：分支AC对接BBC，通过BBC统一配置下发行为管理策略到分支AC。
3. 统一审计：分支AC对接BBC，通过BBC统一配置下发行为审计策略到分支AC。

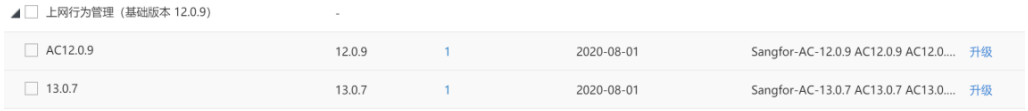
配置步骤

步骤1.分支AC接入BBC。

在BBC[管理]菜单下点击[设备升级]。

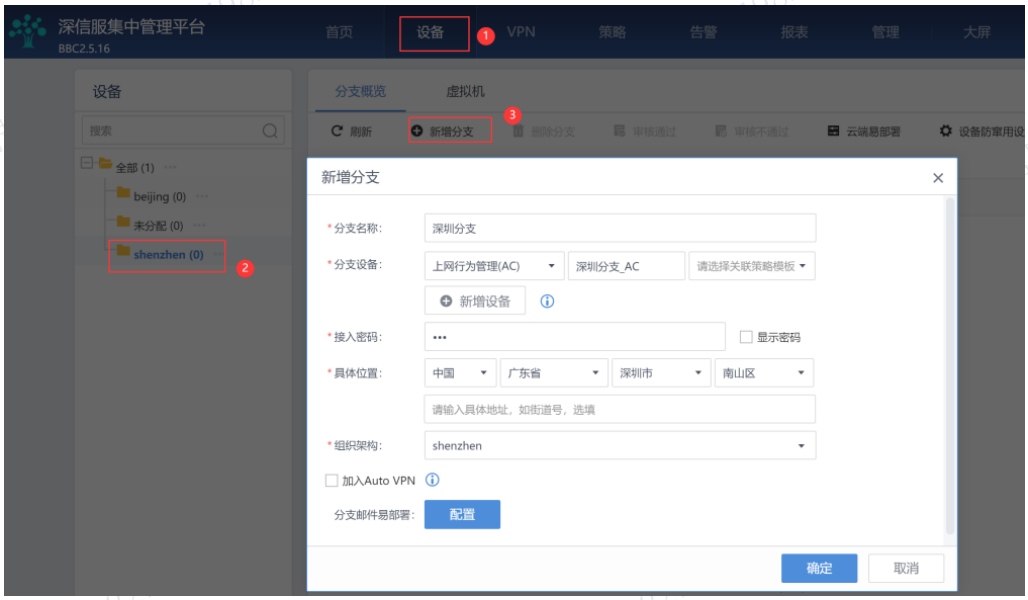
步骤2.选择[分支版本中心]选项卡，点击<新增>，命名版本名称并导入AC对应的BBC镜像。





步骤3.选择[升级包管理]选项卡，点击<新增>导入AC升级包。并在[分支版本中心]选项卡选中AC12.0.9，点击<升级>按钮加载升级包升到AC对应的版本。

步骤4.选择BBC设备菜单左树选中分支区域分组，在[分支概览]中点击<新增分支>，输入分支名称、分支设置、接入密码、具体位置、组织架构。点击<确定>即可。



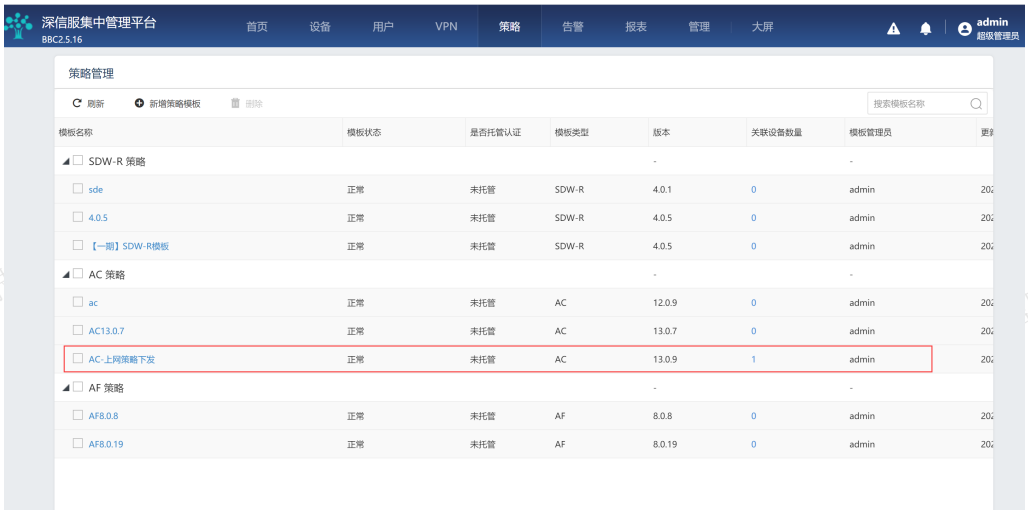
步骤5.在BBC管理菜单上点击<认证中心>配置接入认证中心，勾选开启与认证中心对接，填写认证中心地址、对接密钥、分支访问认证中心地址、认证中心端口、重定向端口、LDAP服务端口、逃生机制。再点击<保存配置>按钮，配置完成后可在用户菜单栏下看到接入的在线分支。

步骤6. 在分支AC[系统管理/系统配置/高级配置/加入集中管理设置]中选择[集中管理平台]为BBC，输入中心端接入地址、接入设备名称、接入密码、共享密钥。

步骤7.在认证中心AC上[接入管理/接入认证/联动对接设置/控制器对接/认证中心设置]中勾选[启用认证中心功能]对接BBC和分支AC，填入接入密钥和通信端口。

步骤8.统一认证下发：

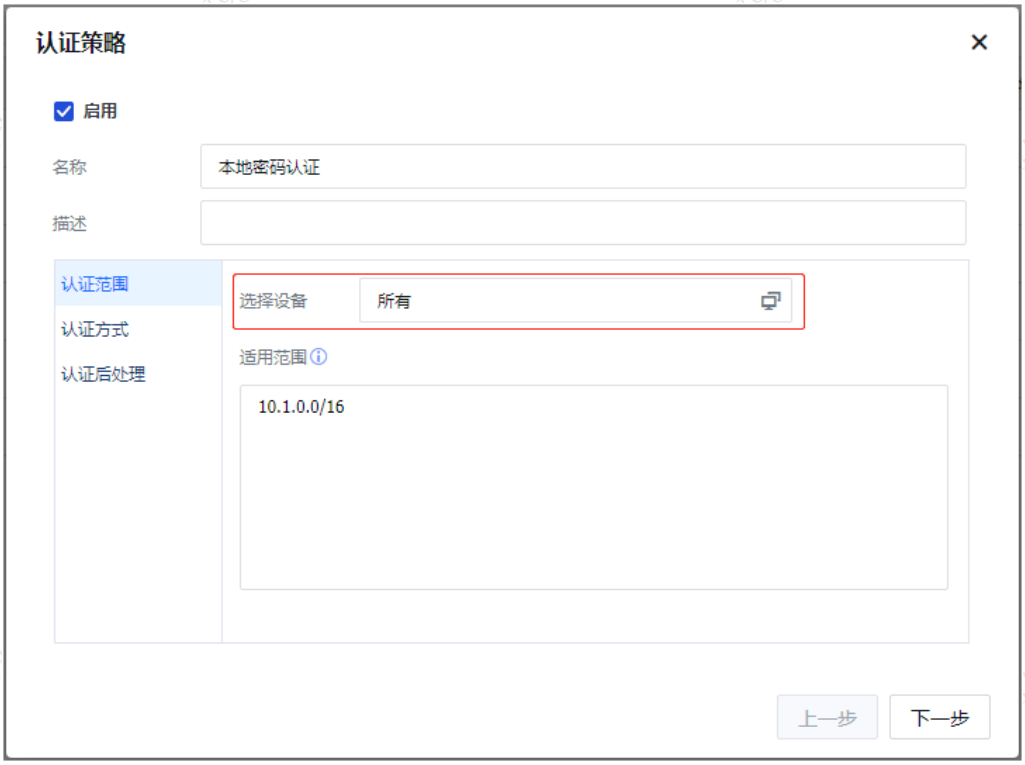
在BBC[策略]菜单栏点击<新增策略模板>，选择配置方式、模板类型、模板版本、模板名称、关联设备。

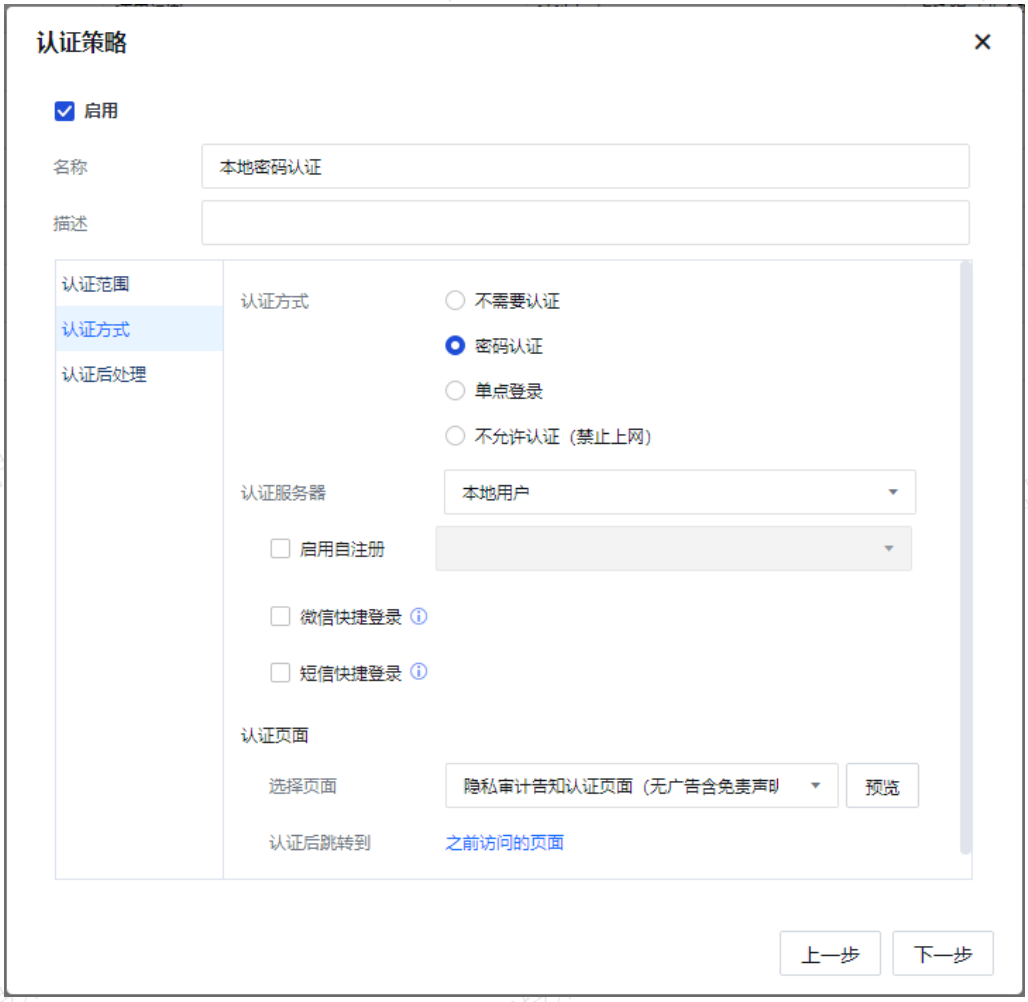


步骤9.在步骤8中点击[AC-上网策略下发]进入AC策略模板中[接入管理/接入认证/认证高级选项/认证托管]查看认证托管模板策略并点击右上角[立即下发配置]下发认证托管策略到分支AC。

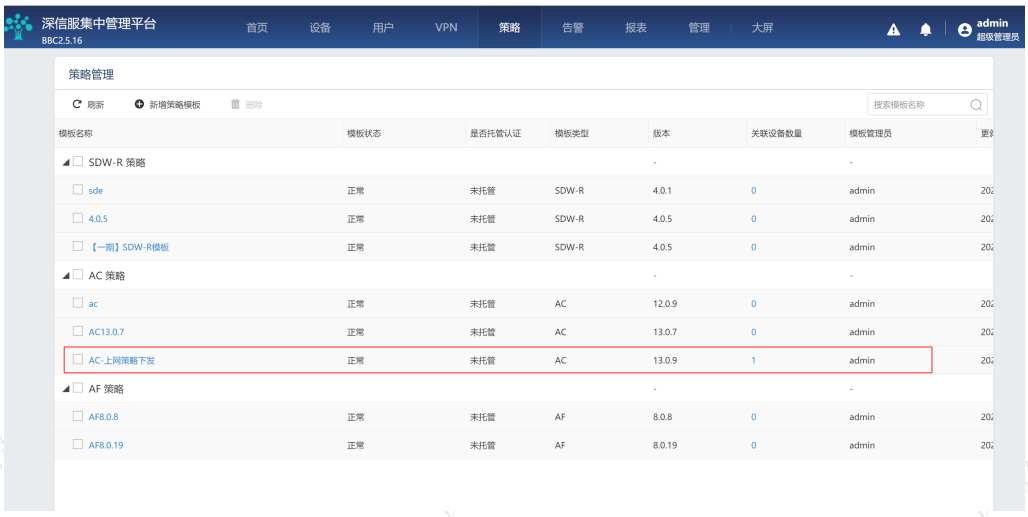
步骤10.在分支AC上[接入管理/接入认证/认证高级选项/认证托管]查看已被下发认证托管策略并接入认证中心。托管成功后认证中心的用户会以域用户的方式存在分支AC中。

步骤11.在认证中心AC上[接入管理/接入认证/PORTAL认证]配置本地密码认证策略，在<选择设备>中选择分支AC，下以选择所有分支AC为例，根据提示点击<提交>完成配置。





步骤12.统一管控，在BBC[策略]菜单栏点击[AC-上网策略下发]进去配置策略模板。



步骤13.在策略模板[行为管理/访问权限策略]新增访问权限策略，勾选[应用控制]，<添加>选择适用应用，勾选[访问网站/新闻用户]。

步骤14.统一审计，在BBC策略模板[行为审计/上网审计策略]中<新增>上网审计策略，勾选审计对象。并点击右上角[立即下发配置]。

效果预览

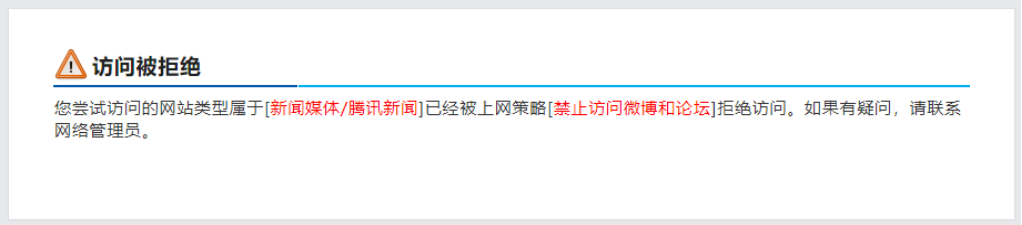
1. 分支AC的用户上网需要通过认证。

2. 认证通过后可以在分支AC上看到用户以域用户所属组上线，在认证中心AC正常上线。

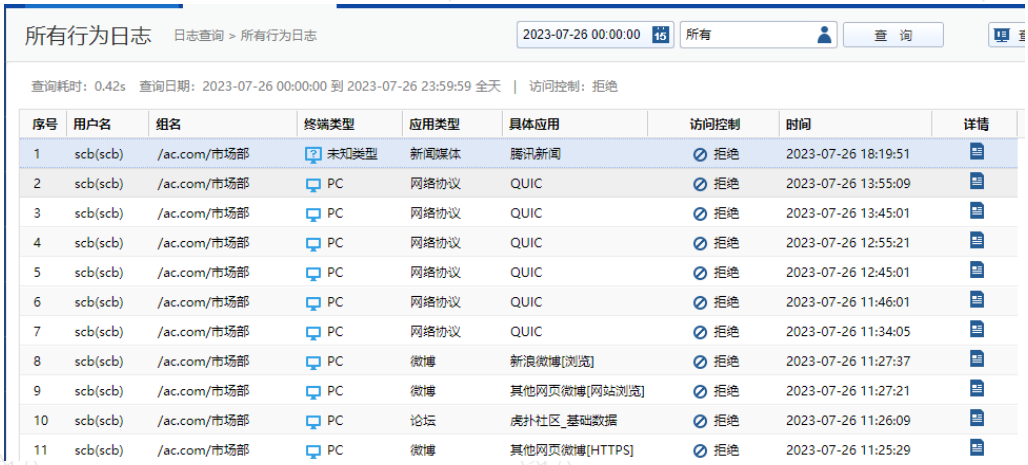
3. 在分支AC上可以看到下发的控制策略。

4. 在分支AC上可以看到下发的审计策略。

5. 终端无法访问新闻门户页面。



6. 在日志中心中审计到网站访问记录。



序号	用户名	组名	终端类型	应用类型	具体应用	访问控制	时间	详情
1	scb(scb)	/ac.com/市场部	未知类型	新闻媒体	腾讯新闻	拒绝	2023-07-26 18:19:51	
2	scb(scb)	/ac.com/市场部	PC	网络协议	QUIC	拒绝	2023-07-26 13:55:09	
3	scb(scb)	/ac.com/市场部	PC	网络协议	QUIC	拒绝	2023-07-26 13:45:01	
4	scb(scb)	/ac.com/市场部	PC	网络协议	QUIC	拒绝	2023-07-26 12:55:21	
5	scb(scb)	/ac.com/市场部	PC	网络协议	QUIC	拒绝	2023-07-26 12:45:01	
6	scb(scb)	/ac.com/市场部	PC	网络协议	QUIC	拒绝	2023-07-26 11:46:01	
7	scb(scb)	/ac.com/市场部	PC	网络协议	QUIC	拒绝	2023-07-26 11:34:05	
8	scb(scb)	/ac.com/市场部	PC	微博	新浪微博[浏览]	拒绝	2023-07-26 11:27:37	
9	scb(scb)	/ac.com/市场部	PC	微博	其他网页微博[网站浏览]	拒绝	2023-07-26 11:27:21	
10	scb(scb)	/ac.com/市场部	PC	论坛	虎扑社区_基础数据	拒绝	2023-07-26 11:26:09	
11	scb(scb)	/ac.com/市场部	PC	微博	其他网页微博[HTTPS]	拒绝	2023-07-26 11:25:29	

说明 :

1.需要保证认证中心AC、BBC、分支AC之间的网络连通性。

2.认证中心AC注意需要开启认证口和开放LDAP接口。

运维管理

本章主要讲解产品的运维管理，为管理员例行维护设备以及简单故障排除提供指导。

日常巡检

维护事项	维护说明
设备搬移	在移动设备前一定要拔掉所有电源线和外部电缆。
设备上架	4. 用户并不具备标准机柜情况下，可将设备安装在干净的工作台上。并保证安装工作台足够牢固，足以承担设备及电缆的重量，设备四周留出10cm散热空间。 5. 不可在设备上放置重物。 6. 在机器上架安装过程中，注意同一机柜中其它设备，避免在安装过程中碰掉其他设备的电源，网线接口等.
设备耳片安装	设备安装托盘或导轨后，可视情况不安装耳片。其他情况都必须安装耳片。
电源接线	有冗余电源设备必须接通冗余电源。
	1. 布放走道线缆时，必须绑扎。绑扎后的线缆应互相紧密靠拢，外观平直整齐，线扣间距均匀，松紧适度。布放槽道线缆时，可以不扎绑。

布线	2. 信号电缆、尾纤、电源线的布放尽量避开，不要靠得太近，更不能绑扎在一起。线缆在机柜中捆扎后，应平直、捆扎整齐，不得有线缆缠绕、弯曲等现象。 3. 尾纤扎绑前检查光纤走线区域附近是否有毛刺、锐边或锐角物体等，如果发现应尽量规避。在机柜外布放时，建议安装光纤保护套管（波纹管）。
标签	线缆必须贴标签注明: 4. 电源线标签：内容为电缆对端位置信息，填写标签所在电缆侧对端设备、控制柜、分线盒或插座的位置信息。 5. 信号线标签：标签两面内容分别标识电缆两端所连端口的位置信息。 6. 粘贴标签之前先在整版标签纸上填写或打印好标签内容，然后揭下、粘贴在电缆或标识牌线扣上。

设备硬件状态检查

SANGFOR AC系列硬件设备正常工作时POWER灯常亮，设备的ALARM灯只在设备启动时因系统加载会长亮（大概1～5分钟），正常工作时熄灭。如果在使用过程中此灯长亮，且设备无法正常使用请按照如下步骤进行操作：

如果设备以双机热备部署时：

1. 备机的ALARM灯会规律闪烁标识当前状态。
2. 立即将主机设备断电关闭，将业务切换到备机；半小时后将设备重启。
3. 若重启设备后ALARM灯仍一直长亮不能熄灭，请速与深信服技术支持工程师取得联系，确认是否设备损坏。

其他部署模式出现故障时请速与深信服技术支持工程师取得联系。

接口指示等检查

正常情况下，网口link灯在网口接线后会呈绿色（百兆链路为橙色，千兆链路为绿色）且长亮，网口ACT灯在有数据通过的时候会呈橙色且会不停闪烁，如果link灯不亮或者act灯不闪（接口左侧的灯为ACT灯，接口右侧的灯为link灯），请按照如下步骤进行操作：

1. 检查网线是否破损；
2. 检查网口水晶头是否有破损；
3. 检查网卡双工模式是否协商匹配；
4. 上述均没有问题，请及时重启设备切换主备，并及时联系深信服技术支持工程师。

设备CPU运行检查

通过设备控制台[首页]的设备状态界面，检查CPU占用率是否长期居高，如果CPU长期居高，请按照如下步骤进行操作：

1. 查看[全网监控/流量分析]的接口吞吐率栏，检查当前带宽是否一直处跑满的状态。
2. 查看[全网监控/流量分析]的业务流量排名栏，检查是否有突发流量很高的用户。
3. 开启设备防内网DoS攻击模块（[安全管理/终端上网安全/安全配置]），检查设备是否遭受到了DoS攻击，防DoS攻击日志，可在[系统管理/系统诊断/系统日志]中查看。

4. 某个进程是否异常。（联系深信服技术支持工程师确认）

设备异常状况检查

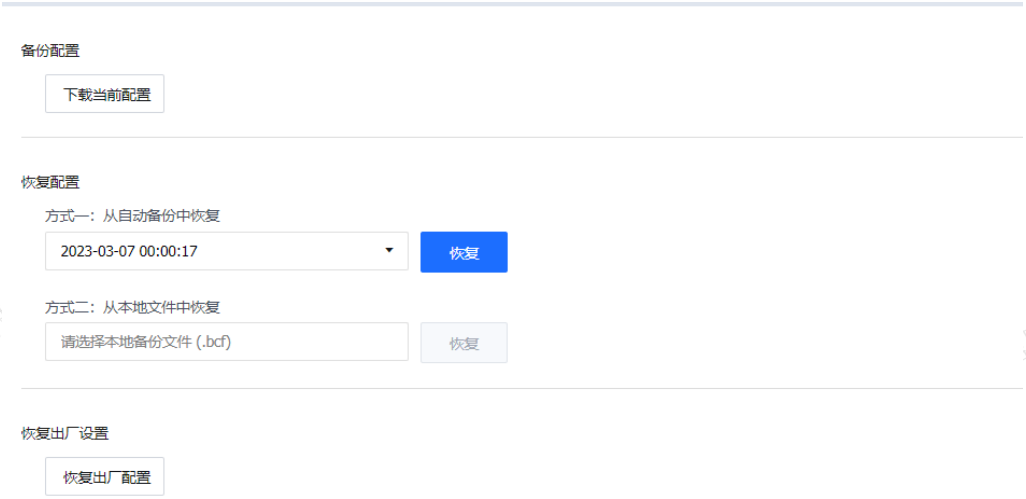
检查设备硬件是否有异常（风扇，硬盘是否有异常声响）如果设备内部有异常声响，可能是硬盘或风扇的异常工作导致，请立即断开电源停止设备工作，如有备用机，请立即将系统切换到备用机；并及时联系深信服技术支持工程师以确认故障并返修设备。

设备配置信息检查

设备配置备份

为了保证网络的稳定运行，建议用户每个月进行一次人工配置备份，以防止AC系统意外瘫痪导致系统无法迅速恢复。

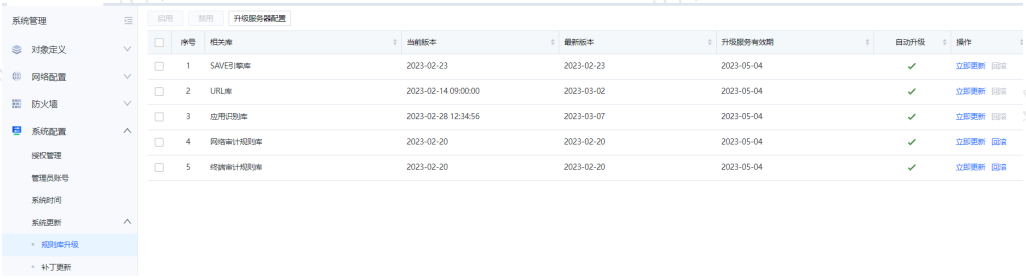
操作方法：登录AC控制台，点击[系统管理/系统配置/配置备份与恢复]，点击<下载当前配置>下载配置并妥善保存即可。



规则库版本检查

为了确保设备能够正常识别最新的网络应用，建议定期检查设备规则库是否更新。

设备在联网的情况下能自动更新到最新的规则库；设备在不联网的情况下选择通过本地导入最新的版本。



设备安全检查

控制台账号安全性检查

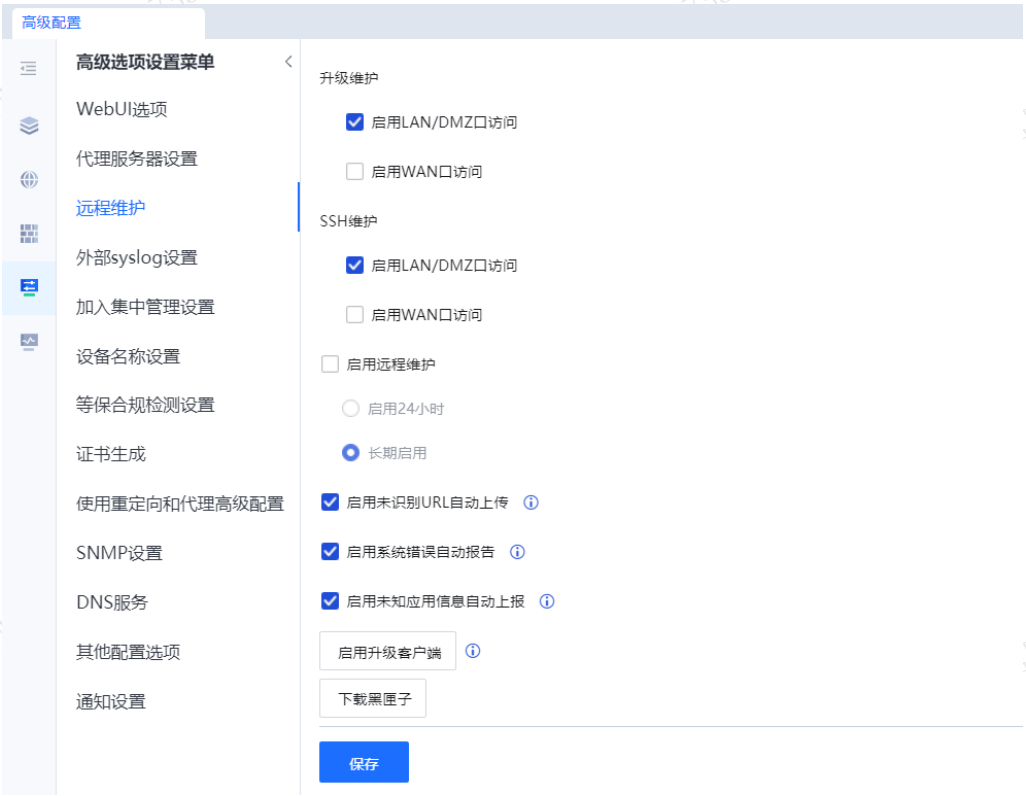
1. 控制台管理员密码一个月内有没有修改过，如果控制台管理员密码一个月内都没有修改过，请立即修改并妥善保

存密码。

2. 控制台是否有多余账号，如sangfor、test以及公司英文等不必要的简单账号，如果有的话，请删除多余账号，仅保留授权的管理员账号。

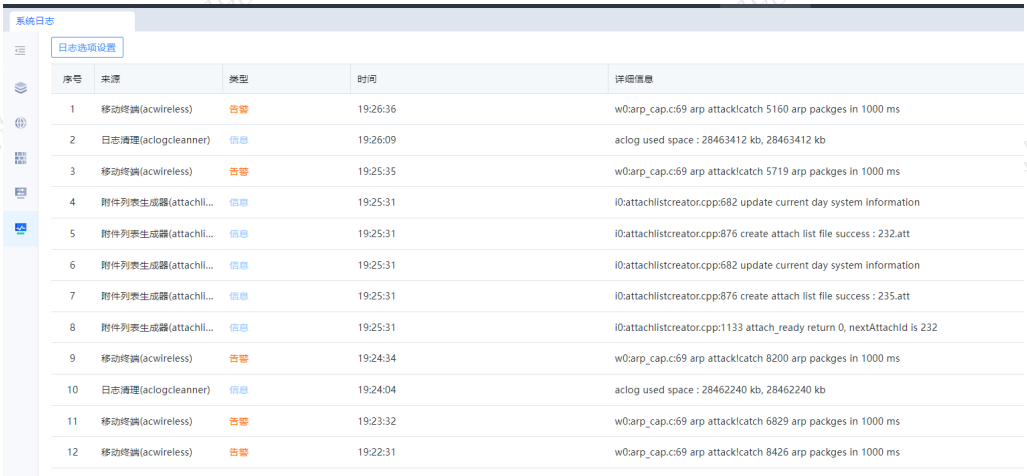
控制台远程维护检查

通过[系统管理/系统配置/高级配置/远程维护]，检查设备远程维护状态是否开启，避免设备被非法人员从WAN口接入设备。

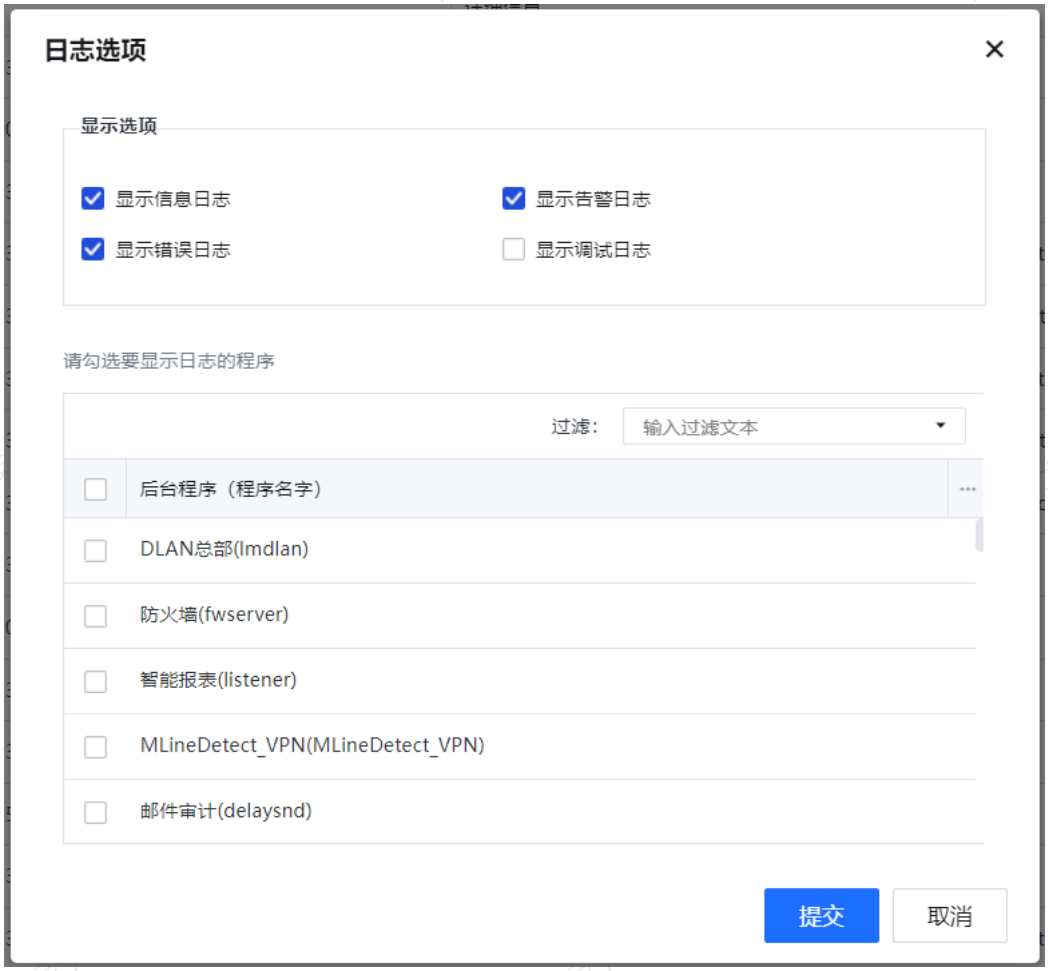


设备日志信息检查

通过[系统管理/系统诊断/系统日志]，可以看到设备各模块运行状态日志，可通过日志判断设备各模块是否正常运行。



系统日志包含信息、告警、错误、调试四个级别，点击<日志选项设置>，可以过滤需要查看的级别以及模块的日志。



如果系统日志中出现大量错误日志和告警日志，请及时联系深信服技术支持工程师，确认是否设备程序运行故障。

设备健康检查

管理员可以在对设备进行检查，点击<检查>会对设备进行巡检，然后下载报告即可看到设备当前的健康信息状态。

下载报告可以查看设备巡检结果，包括设备巡检的概况、设备负载的情况、网络连通性、系统运行状态、核心进程检查、版本历史重大BUG/补丁检查、规则库情况。

设备配置和密码恢复

交叉线恢复密码

由于admin密码丢失，没有其它账号可以使用，导致无法登录控制台及后台，可以进行交叉线恢复密码。

操作步骤

步骤1.确保电脑和设备可以通信，访问设备地址https://网关IP/php/rp.php，提示“创建文件成功，请连接交叉线并重启设备”。

步骤2.访问此地址不需要登录控制台，访问此地址作用是创建一个标记文件，如果交叉线短接了两个电口，设备重启时，会判断标记文件是否存在，存在则执行恢复密码流程，不存在，则执行恢复出厂设置流程。

步骤3.准备交叉线将任意两个电口短接。（通常使用ETH0和ETH1口短接。AC12.0.12及之后的版本需要用ETH0口和ETH2口对接）

步骤4.手动重启设备，重启过程中，注意观察交叉线短接的两个电口ACT灯状态，两个电口ACT灯同时闪烁10次后，说明密码恢复完成，此时可以拔掉短接的交叉线，通过默认的控制台账号密码admin/admin登录设备即可。设备重启到密码恢复成功大约3到5分钟左右。

步骤5.如果步骤2和步骤3无法根据网口灯状态判断密码恢复是否成功，可持续等待5-10分钟过后，尝试通过默认账号admin/admin账号登录设备。

U盘恢复密码

在U盘里分别放入对应功能名称的txt文件，通过将U盘插入设备的USB口来实现U盘恢复控制台密码。全网AC从标准版本13.0.4开始支持U盘恢复密码。

1. 新建一个txt文档，将其重命名为reset-cfg.txt，将txt文档拷贝到U盘根目录，U盘格式为FAT 32的。
2. 确保电脑和设备可以通信，访问设备地址 https://ACIP/php/rp.php，会有提示“创建文件成功，请连接交叉线并重

启设备”。注意：请将“网关IP”改为您的设备的IP地址，此步骤不成功时会导致恢复出厂设置。

3. AC上插入U盘，重启设备。

4. 当设备的alarm红灯熄灭之后开始闪烁即恢复密码成功，拔出U盘。

⚠ 注意：

U盘恢复密码，需要设备重启。

控制台恢复出厂配置

设备可以正常登录，希望将设备恢复出厂状态，可直接在设备WEBUI控制台直接恢复。

登录AC控制台，点击[系统管理/系统配置/配置备份与恢复]，点击<恢复出厂设置>，根据提示操作即可。

交叉线恢复出厂配置

不知道设备地址，升级客户端也无法搜索到，可尝试交叉线恢复出厂设置后登录设备。

步骤1.准备交叉线将任意两个电口短接。

步骤2.手动重启设备，重启过程中，注意观察交叉线短接的两个电口ACT灯状态，两个电口ACT灯一直同时闪烁，说明出厂设置恢复完成，此时拔掉短接的交叉线，设备会自动重启，设备启动后，通过默认地址及默认账户登录设备。重启到配置恢复成功大约5分钟左右。

步骤3.如果第二步无法根据网口灯状态判断出厂配置是否恢复成功，持续等待直到设备重启，设备重启时，务必要拔掉交叉线（如果没有拔下交叉线，设备会循环重启）。设备启动后，通过默认地址及默认账户登录设备。整个过程大约10分钟左右。

⚠ 注意：

1. 交叉线恢复密码或出厂设置，设备都需要重启，需要提前和用户说明，建议将设备下架操作。

2. AC/ SG12.0.12以上版本，请使用交叉线短接ETH0和ETH2来恢复默认密码。

补丁更新指导

深信服补丁获取方式

深信服针对不同的场景提供了五种补丁获取方式：

1. 设备能与在线补丁服务器连通时：自动获取补丁；
2. 设备通过代理服务器访问外网时，配置代理服务器获取补丁包；
3. 设备无法访问外网时，通过深信服OLU内网补丁服务器获取补丁包；
4. 设备不能与在线补丁服务器连通，但是访问设备控制平台的PC可以上网时：通过PC浏览器访问深信服在线补丁服务器获取补丁；
5. 设备不能与在线服务器连通，且本机PC无法上网时：可使用手机扫描二维码方式获取离线补丁。

检查环节

确认设备联网情况，分为以下5种：

1. 设备正常联网，可以直接访问深信服在线补丁服务器；
2. 设备无法直接访问网络，但能使用代理上网获得规则库更新；
3. 设备离线但能使用“**OLU内网补丁服务器**”获得补丁更新
4. 设备离线但访问设备的PC可以联网，且不支持使用“**OLU内网补丁服务器**”；
5. 设备以及访问设备的PC均完全离线，且不支持使用“**OLU内网补丁服务器**”。

确认升级服务器设置，用户可以通过以下三种方式设置升级服务器：

1. **手动输入服务器地址：**手动输入OLU内网补丁服务器地址，则可以从OLU内网补丁服务器中获取补丁更新。(OLU内网补丁服务器只支持补丁更新，暂不支持规则库更新)
2. **自动选择服务器地址：**设备会在深信服支持的在线升级服务器中轮询，自动选择一个最优的服务器获取更新信息。
3. **选择特定的服务器地址：**指定从特定的在线补丁服务器上获取更新信息。

场景介绍及配置

本文档中相关配置会以AC设备的配置做示例，其他的产品配置方法大致相同。

设备能联网且开启补丁自动更新

设备能联网且开启补丁自动更新，那么无需用户操作，用户可查看已经更新的补丁。

管理员进入[系统管理/系统配置/系统更新/补丁更新]补丁更新页面，查看更新的补丁。

设备能联网且未开启补丁自动更新

设备能联网且未开启补丁自动更新，那么设备可以自动获取更新补丁，但是需要用户操作，才能安装补丁。

1. 管理员进入[系统管理/系统配置/系统升级/补丁更新]补丁更新页面，查看补丁更新列表；
2. 点击<一键安装>，执行补丁安装。
3. 查看补丁是否成功安装。

⚠ 注意：

建议用户自动[补丁自动更新]功能，涉及到重启设备或者其他特殊场景的补丁更新时会提醒客户，需要手动确认后才会执行此类补丁的更新。

设备通过代理服务器获得补丁更新

若设备不能联网，但是内网有可以代理上网的服务器，那么可以通过设置代理服务器，使设备通过用户内网的代理服务器上网更新补丁。

在配置完代理服务器后，且设备通过代理服务器能正常访问外网后，设备获取补丁包的方式则和场景一、二无任何区别，此章节仅介绍如何配置代理服务器。

1. 进入[系统管理\系统配置\系统更新\代理设置]功能菜单栏。

2. 勾选[启用代理服务器]，填写代理服务器的IP地址、端口。如果连接代理服务器需要用户名和密码，则勾选[验证用户]输入代理服务器需要验证的用户名和密码（此部分的信息由客户提供）

设备不能联网但访问设备的PC可以上网

设备不能与在线补丁服务器连通，但访问设备控制台的PC可以上网时：通过PC浏览器从深信服在线补丁服务器上获取补丁。

1. 管理员通过首页提醒，或者补丁更新页获取更新的补丁检测。（用户登录设备的控制台后都会有提示）
2. 通过补丁更新页获取补丁：点击[补丁更新]界面的<获取离线补丁包>按钮。

3. 管理员下载补丁到本地，再通过<手动上传安装>将下载的补丁上传到设备安装。

设备不能联网且PC不能联网

设备不能与在线服务器连通，且访问设备的PC无法上网时，可使用手机扫描二维码方式获取离线补丁。

1. 用户可以在登录首页或者补丁更新页，点击<获取离线补丁包>，用手机扫描弹出窗口里的二维码，复制链接下载补丁更新。

获取补丁包方式

方式一 设备能与在线补丁服务器联通时：自动获取更新补丁

方式二 设备不能与在线补丁服务器联通，但本地PC能上网时：通过PC浏览器从在线补丁服务器上获取

检测补丁更新

方式三 设备不能与在线服务器联通，且本地PC无法上网时：您可使用手机扫描下方二维码获取离线补丁包，然后通过【手动上传安装】按钮进行安装；或电话联系技术服务400-005-5530

刷新二维码

2. 用户可以将下载的补丁传到PC后，进入补丁更新页，在手动安装，并查看补丁安装成功的情况。

辅助工具使用

上网故障排除

当用户上网的流量经过AC设备出现异常时，可通过AC的上网故障排除功能查询该用户的数据包在通过AC设备时被拒绝的原因，便于快速定位故障原因。上网故障排除页面提供[直通排障]和[设备搬包]（搬包功能仅路由和网桥模式下可使用）两种故障排除手段。

直通排障

直通排障一般用于测试上网异常IP是否由AC设备拦截造成。针对上网异常的IP开启直通后，如果AC相关功能模块对该IP进行了拦截阻断，则会在直通日志终打印出被拦截的原因以及对应的功能模块，管理员可根据直通日志可快速定位问题。

设备上架时为了避免影响业务，可以开启直通，当出现终端异常断网的情况下，可以通过直通排障的日志快速定位问题并恢复业务。

点击<设置并开启>，出现设置开启条件界面，可设置各种过滤条件，包括[拦截日志过滤条件]和[同时开启数据直通]，如下图。

拦截日志过滤条件：用于设置对指定的IP地址开启拒绝列表，默认包括所有网段。

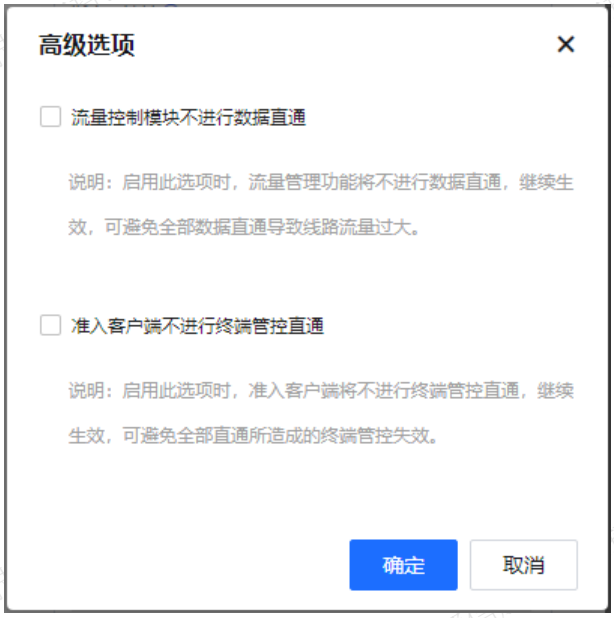
点击<协议条件>，可根据协议类型和端口范围过滤拦截日志，如下图。

协议类型可选择：所有、TCP、UDP、ICMP和其他五种类型。

勾选[提高拦截日志的可读性]，将通过中文显示拦截日志；如果此项不勾选，则通过英文显示拦截日志。

勾选[同时开启数据直通]，可设置开启直通的IP地址或者地址段。此时对于这些IP地址设置的上网策略将不生效，原本策略设置拒绝的数据包会被设备放行。

点击<高级选项>，可设置对流量控制模块和准入客户端策略是否开启直通。如果勾选<流量控制模块不进行数据直通>，则流量管理策略仍然生效，可以避免由于全部数据直通导致流量过大，对用户上网环境造成影响；如果不勾选，流量管理策略将不生效，用于定位被流量控制模块拦截的情况。如果勾选<准入客户端不进行终端管控直通>，则已下发到终端的准入策略（基于准入客户端的策略）仍然生效，可以避免终端安全基线检查失效，终端管控失效；如果不勾选，下发到终端的准入策略不生效，用于定位被准入模块拦截的情况。



当前操作状态：将显示直通和拦截日志的开启情况，如下图。

点击<关闭>，关闭拦截日志和直通。点击<立即刷新>查看拦截日志，数据包被拦截的情况，如下图。

序号	时间	源->目标	协议	设备	大小	线路	应用名称	应用规则	源	丢包标记	动作
1	18:15:42	11.11.11.34:4607 -> 100.1	tcp	eth2 -> NULL	54(B)	线路1	自定义应用_自定...	公司邮件	authv	DROPFL...	Auth policy logic(Acode) dropped
2	18:15:42	100.100.24.200:80 -> 11.1	tcp	eth0 -> NULL	66(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) throw
3	18:15:39	11.11.11.21:4620 -> 100.1	tcp	eth2 -> NULL	54(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) dropped
4	18:15:39	100.100.24.201:443 -> 11.	tcp	eth0 -> NULL	54(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) dropped
5	18:15:31	11.11.11.34:4607 -> 100.1	tcp	eth2 -> NULL	54(B)	线路1	自定义应用_自定...	公司邮件	authv	DROPFL...	Auth policy logic(Acode) dropped
6	18:15:31	100.100.24.204:80 -> 11.1	tcp	eth2 -> NULL	54(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) dropped
7	18:15:31	11.11.11.30:4616 -> 100.1	tcp	eth2 -> eth0	54(B)	线路1	0	0	web aut...	DROPFL...	(line:760)this packet had been dropped
8	18:15:31	11.11.11.30:4616 -> 100.1	tcp	eth2 -> NULL	54(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) dropped
9	18:15:26	11.11.11.30:4616 -> 100.1	tcp	eth2 -> NULL	54(B)	线路1	0	0	authv	DROPFL...	Auth policy logic(Acode) dropped
10	18:15:26	11.11.11.24:4617 -> 100.1	tcp	eth2 -> NULL	1514(B)	线路1	自定义应用_自定...	公司邮件	authv	DROPFL...	Auth policy logic(Acode) dropped

说明：

1. 拦截日志和直通功能开启后，如果管理员未手动点击<关闭>，即使设备重启，仍然是开启状态。
2. 审计策略在开启直通也依旧生效。

设备搬包

搬包功能是AC设备在路由模式和网桥模式下提供的一种紧急逃生的能力，当设备功能模块异常影响业务时，可通过搬包功能直接放开对流量的流量的控制从而保证业务流量不中断。

AC设备开启搬包时CPU、内存、IO等资源占用将大幅降低，经过AC设备的数据会被直接转发，不再受任何策略影响(认证策略、访问权限策略、流控策略、上网审计策略等)。

与直通、全局排除功能相比，搬包生效时所有数据包会被直接转发，不会匹配任何策略逻辑，不会生成任何策略管控日志，搬包是一种更彻底的流量放通机制。

在开启搬包功能时，可以选择对所有流量进行搬包，也可以对指定条件的流量进行搬包（如下图所示）。

说明：

1、必需由设备处理的核心逻辑不受搬包影响，具体为：源地址转换(NAT代理上网)、目的地址转换(端口映射)、代理上网流量转发(上网代理)、路由转发；

3、部分特殊流量不支持搬包，如：广播包、组播包；

4、开启搬包时，开启功能前已存在的连接不支持被搬包，这部分连接将继续受策略管控；

5、关闭搬包时，关闭功能前已在搬包的连接不支持退出搬包状态，搬包状态将持续到连接销毁；

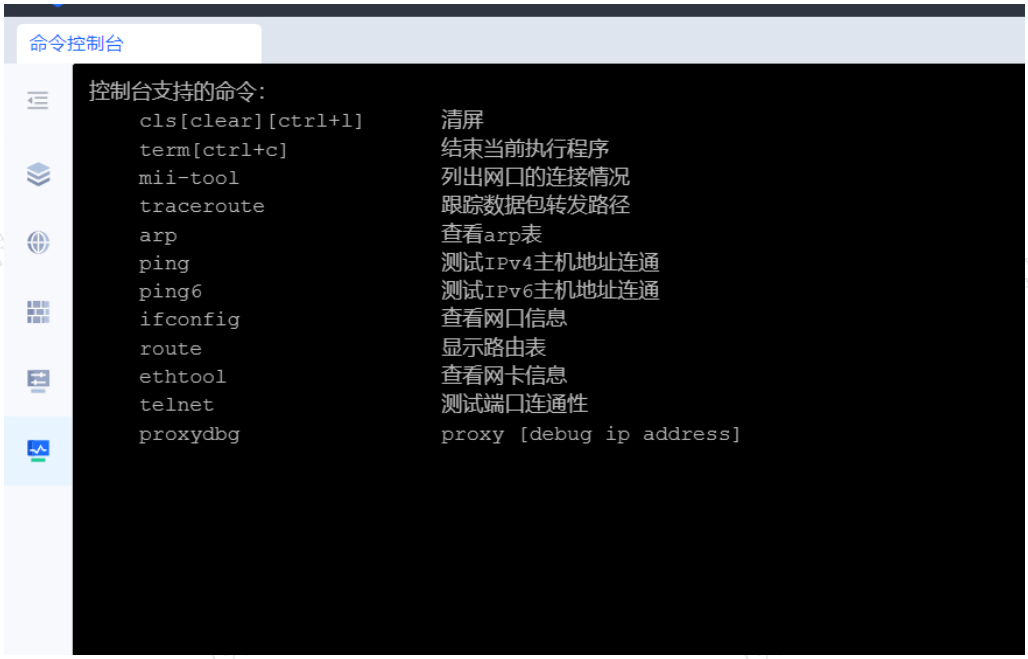
6、子连接将会直接继承父连接的搬包控制状态，即父连接被搬包则其对应的子连接也会被搬包，反之父连接没有被搬包其对应的子连接也不会被搬包；

7、开启搬包后，会出现客户端自动找网关失败、客户端获取准入策略失败、防Dos攻击拦截异常等情况。

命令控制台

全网行为管理设备控制台的[命令控制台]提供一个简单的命令行界面，可对设备的一些简单信息进行查看，支持的命令包括：

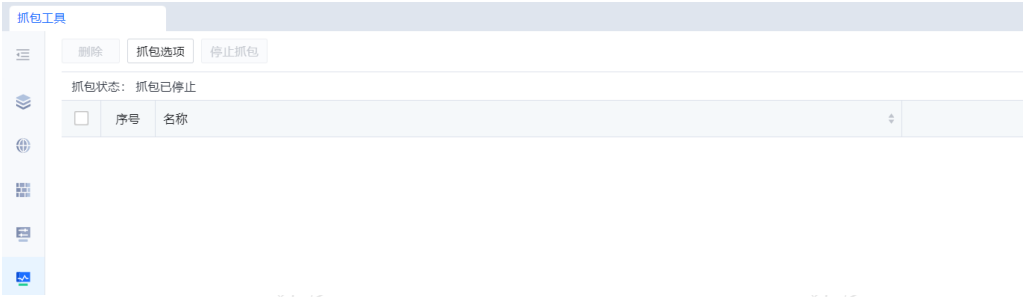
- arp（查看设备的arp表）
- mii-tool（查看设备网口的连接情况）
- ifconfig（查看设备网口信息）
- ping（测试主机地址的连通性）
- telnet（测试端口连通性）
- ethtool（查看设备网卡信息）
- route（显示设备的路由表）
- traceroute（跟踪数据包转发路径）



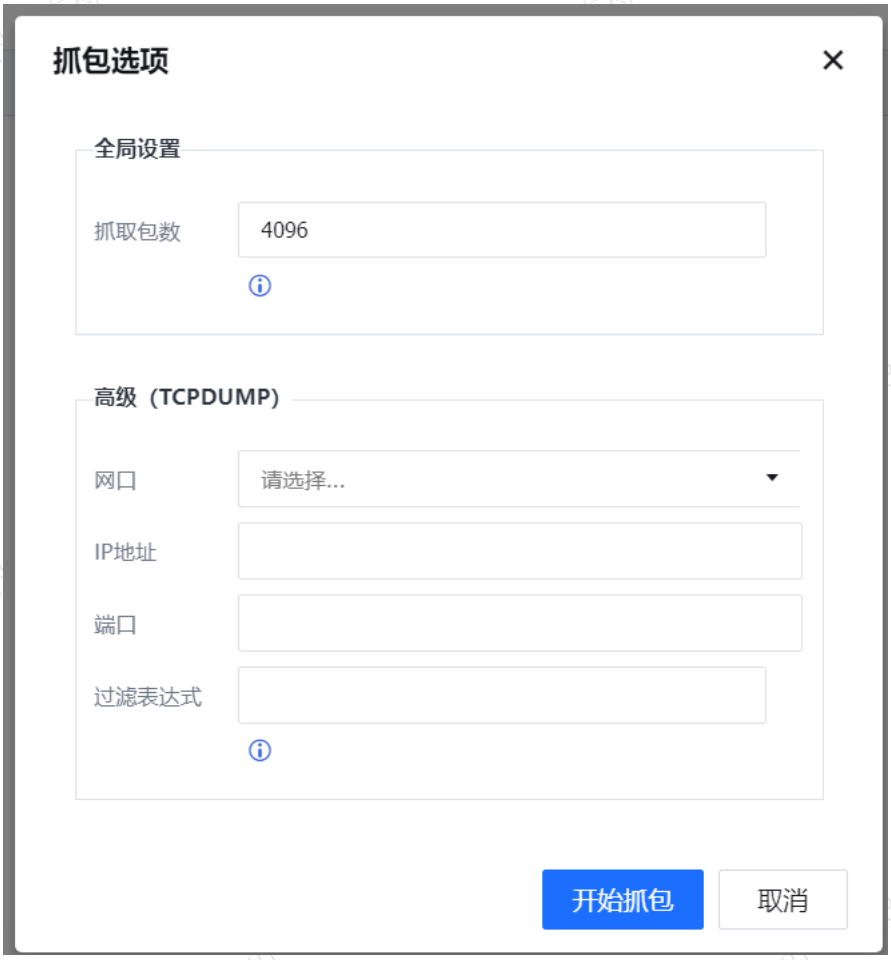
在[系统管理/系统诊断/命令控制台]页面直接输入命令回车即可，ping、telnet、traceroute命令用法和PC相同。

抓包工具

[系统管理/系统诊断]栏的抓包工具以TCPDUMP的方式抓包，将抓取的数据包保存在设备的控制台界面，需要在电脑上安装Wireshark或Sniffer之类的抓包软件，才能打开此数据包进行分析。抓包工具能抓取所有通过设备网卡的数据。

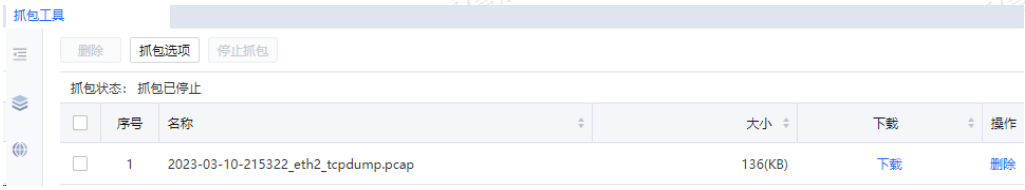


在[系统管理/系统诊断/抓包工具]页面，点击<抓包选项>，选择抓包数量（最大4096个）和网口，设置抓包条件。



过滤表达式同标准tcpdump命令相同，如需要抓192.168.1.100，端口80的数据包的过滤表达式写法如下：host 192.168.1.100 and port 80。

点击开始抓包后，设备开始抓包，抓取的数据包可以从页面下载下来。



升级客户端

升级客户端（网关升级与备份系统v6.2）是深信服开发的用于调试深信服设备的一个客户端工具，集成了设备升级、设备配置备份以及一些常用的网络命令等功能，当出现设备web控制台登录设备异常或不方便使用web登录控制台时，可使用该工具进行一些常见的网络命令测试，下载地址：

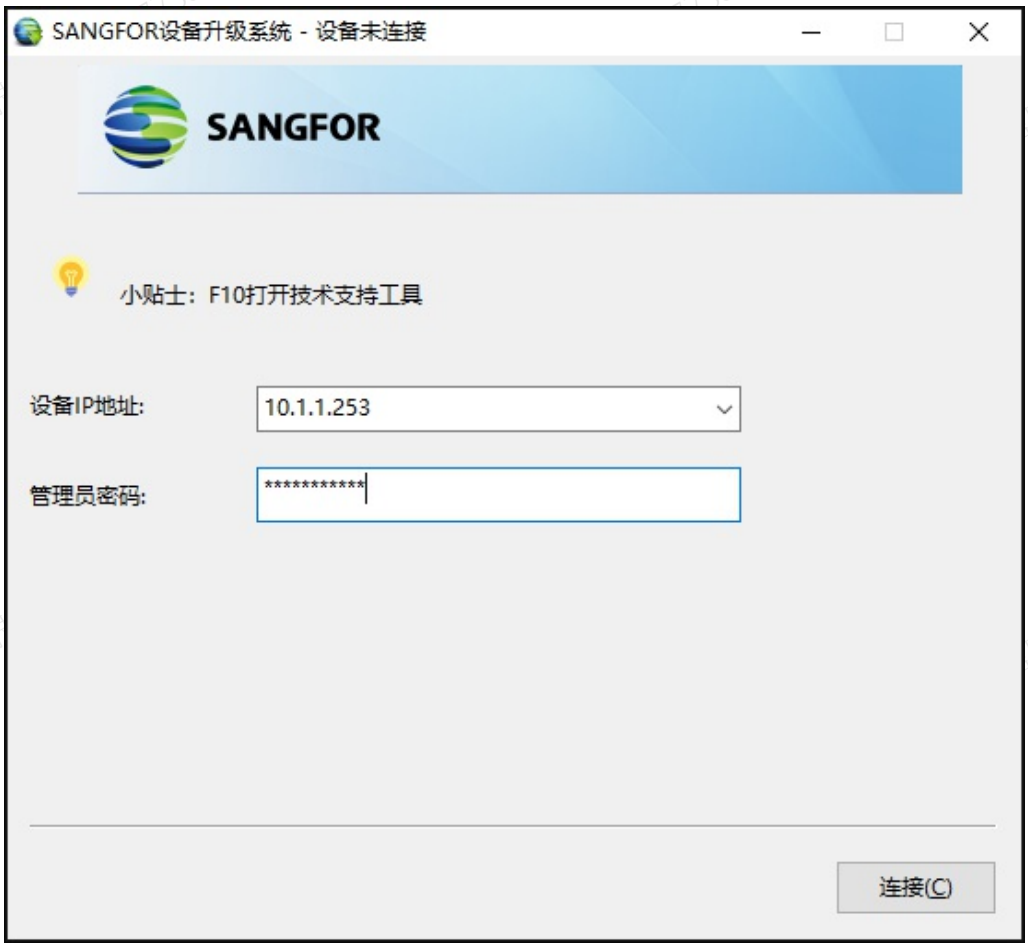
https://bbs.sangfor.com.cn/plugin.php?id=service:download&action=tool

⚠ 注意：

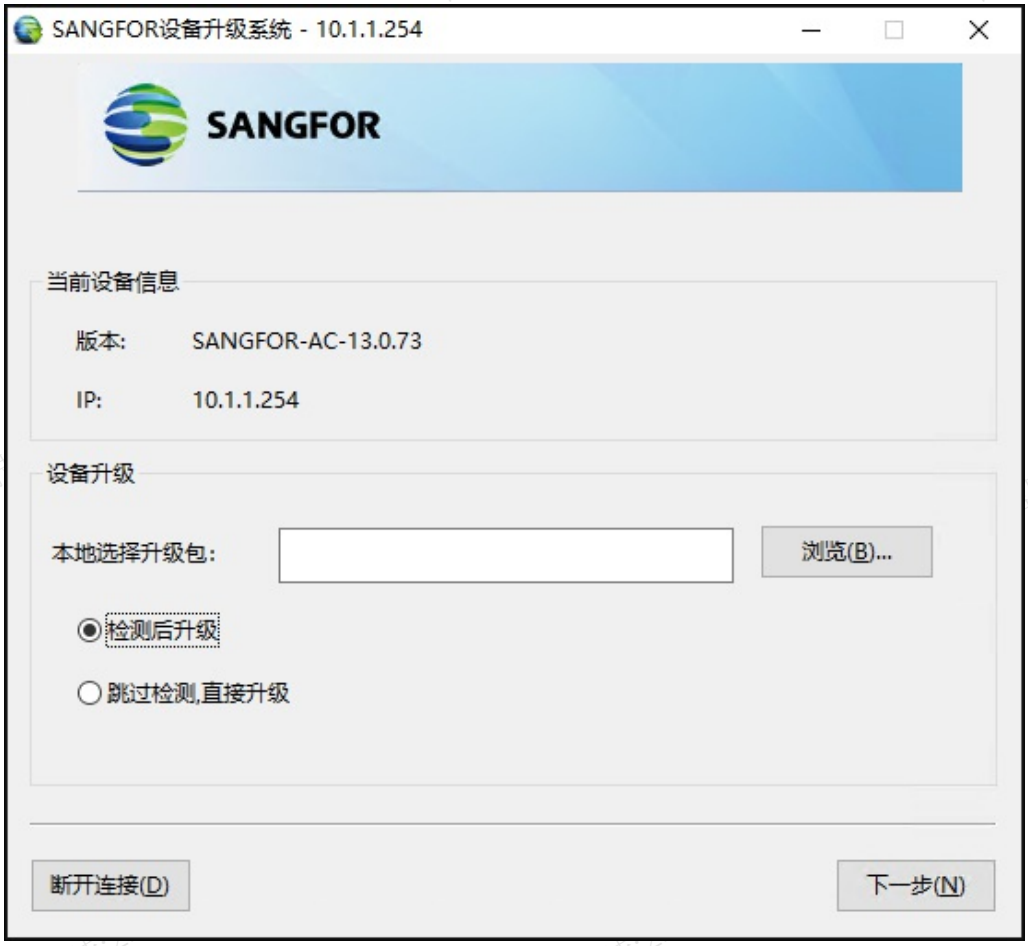
1.使用升级客户端登录设备须放通终端访问设备的TCP51111端口。

2.使用升级客户端前，需要在AC设备[系统管理/系统配置/高级配置/远程维护]中启用升级客户端。

步骤1.SANGFOR_Updater6.2下载完成后，解压即可使用，在解压缩的文件内找到“SANGFOR Firmware Updater.exe”双击运行，即可打开升级客户端接入程序。



步骤2.输入设备IP地址和管理员（admin账号）密码，即可连接设备。



步骤3.从本地加载升级包可升级设备，升级设备请在技术支持工程师的指导下操作。按键盘<F10键>，可调出技术支持工程师工具。

步骤4.命令模块还能选择Ping、查看路由表、查看ARP表、查看网络配置、网卡操作、设备健康状态检查选项。

常见问题排查

故障监控中心

在[系统管理/系统诊断/故障监控中心]里有网络故障排查、用户认证故障排查、客户端解密故障排查、权限策略故障排查、web访问质量监测和单用户检测六个部分。用于帮助运维人员、技术支持工程师等专业人士进行故障自查。

网络故障排查

网络故障排除是用来监控网络的状态，当网络出现异常时，识别错误类型，并提供解决方案。目前可以识别4种网络异常。

3. [内网DOS攻击]

事件说明：内网DOS攻击事件xx次，攻击流量会导转发设备性能超限、线路拥塞，造成上网卡慢或者无法访问网络。

错误类型：内网DOS攻击。

解决方案：请检查网络拓扑变化，是否构成环路。请隔离对应IP设备并对该设备进行病毒查杀。

4. [网口丢包异常]

事件说明：网口丢包事件xx次，网口丢包、错误包会造成上网卡慢，影响用户上网体验。

错误类型：rx_crc_errors。

解决方案：该错误表明数据包传输物理层故障。请更换连接对应网口的网线，或者更换和网线直连的对端网口。

5. [ARP异常]

事件说明：ARP异常事件xx次，设备网关存在ARP无回复或回复异常。

错误类型：ARP异常。

解决方案：请检查网关设备的运行状态及连通性。

6. [网关PPS异常]

事件说明：设备PPS超限事件xx次，PPS造成设备所有控制和审计功能失效。

错误类型：网关PPS异常。

解决方案：设备持续PPS超限表明当前设备性能不足，建议对经过设备的流量进行分流，或者联系商务渠道更换更高端平台设备。

⚠ 注意：

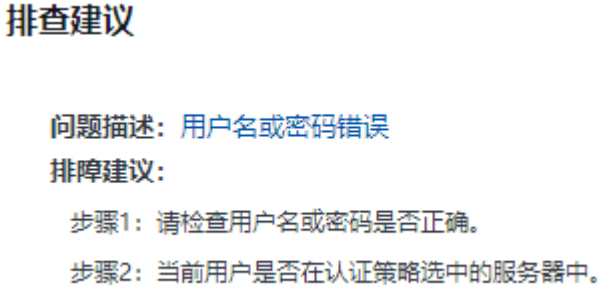
AC以网桥模式部署时才支持网关PPS异常检测。

用户认证故障排查

管理员利用“用户认证故障排查”工具可以自查用户出现认证异常无法上网、上线错误等异常问题。在[用户认证故障排查]界面可以查看设备记录的用户认证过程中出现的异常情况，方便运维人员快速定位问题。

管理员在输入框输入异常用户的用户名/IP/MAC地址，点击<搜索>，即可看到该用户认证过程中的异常情况。

管理员在排障建议列表点击<详情>能弹出排障建议。



管理员可查看问题描述：如“用户名或密码错误”，参考排障建议步骤去排查问题。

单用户检测

“单用户检测”工具包含[终端重定向检测]和[准入客户端日志检测]。

终端重定向检测

当整体网络质量判定不能解决问题时，可以对单用户进行针对性检测。

例如：在发现用户A的在上网慢的列表中，可以在单用户检测—检测对象中输入用户名或IP地址或者点击选择用户在下列组织结构中勾选用户。

7. 点击<选择用户>，在设备用户组织结构中选择指定用户。

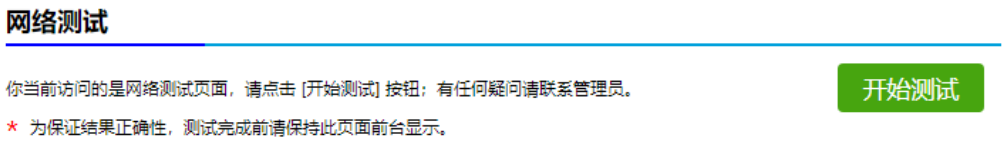
8. 确定<提交>后，在监测地址点击<设置>，设置监控地址。

9. 终端页面重定向：可以选择访问百度是重定向到测试页面或者所有web访问重定向到测试页面。

10. 监视地址：可以选择使用内置监测地址库或者自定义监测地址。

11. *确定<提交>后，点击开始设置，以www.baidu.com为例。*

12. 用户访问www.baidu.com，重定向到测试页面。



13. 点击<开始测试>后，用户开始检测。测试时会有时间提示。

14. 管理员页面显示开始检测。

15. 用户检测完毕。

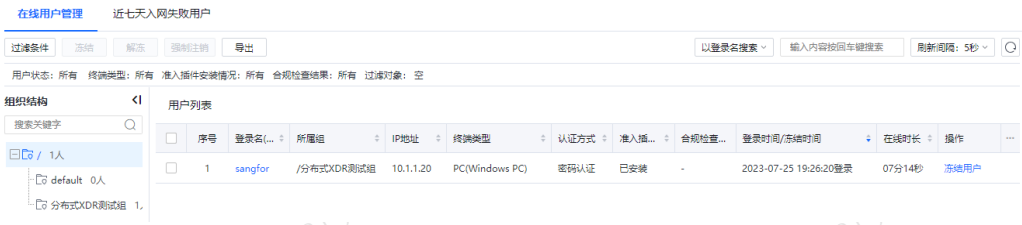
16. 管理员页面显示检测结果。

准入客户端日志检测

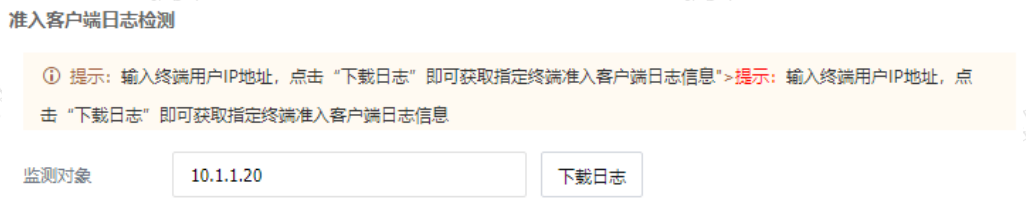
通过在Web控制台收集用户终端上的准入客户端日志，无需使用U盘、远程工具等方式从用户终端拷贝准入客户端日志，从而提高管理员排障效率。

例如：企业部署了AC设备，为满足企业办公安全，配置了终端检查策略。当员工反馈终端PC异常，管理员无法只根据AC设备提供的准入安全日志定位问题时，需要结合终端PC上的准入客户端日志更深层次地分析、定位问题，可直接在AC设备Web控制台下载指定监测对象的准入客户端日志。

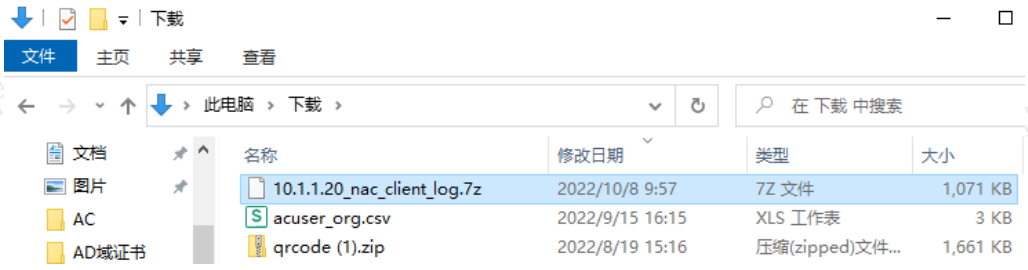
17. 在[全网监控/入网用户管理]查看员工信息，确认用户已上线，并安装准入插件。



18. 在[全网监控/故障监控中心/单用户检测]中的“准入客户端日志检测”工具填入监测对象IP，点击<下载日志>。



19. 下载完成后可在本地查看日志文件



客户端解密故障排查

客户端解密故障主要根据准入客户端的安装情况、证书安装情况、异常详情来定位故障信息。

其中排查思路如下：

• 匹配解密策略：若客户端解密故障排查中没有该用户信息或匹配解密策略为空，检查解密策略是否已经匹配且匹配正确。

• 准入客户端的安装情况：

未安装：该用户未安装准入客户端，检查终端准入客户端安装运行情况，可手动安装。

已安装：该用户已安装准入客户端。

• 证书情安装情况：

证书安装成功：该用户已安装证书成功。

其他状态包括：系统证书安装失败、火狐证书安装失败、证书安装失败、证书无效、证书过期。

• 异常情况：

代理正常运行：状态正常。

代理异常：准入客户端代理无回包。

驱动异常：包括驱动文件不存在、驱动签名失效、驱动被杀毒软件阻止、基本筛选引擎（BPE）服务被禁止。

权限策略故障排查

通过“权限策略故障排查”可以查看用户访问权限策略匹配情况，当策略匹配的用户与实际期望不符合时，运维人员或工程师可以使用该功能进行排查。

管理员在输入框输入异常用户的IP地址，点击<开始监测>，可以看到该用户匹配到的所有策略。通过与实际需求进行比对，找到异常点并调整策略。

管理员可以在应用类型中选择需要查找的相应策略，点击<匹配详情>，可显示该IP 对应的策略名称、策略控制序号、匹配维度、匹配结果等信息，可根据这些信息找到异常点来调整策略信息。

解决方法：识别到该策略的DNS协议没有放通，导致访问所有的网站都拒绝，回到权限策略设置把DNS协议去掉勾选，就能访问正常。

Web访问质量监测

用于显示内网终端访问监测网站的网络质量。以 HTTP（默认所有网站）与HTTPS（用户自定义网站）请求作为网络质量检测的评估对象，对核心指标（RTT时延、DNS时延、TCP重传率..)进行抽样，根据质量分析数据模型来对所有上网IP进行质量评估，结果分两类：优、差，并按单用户的网络质量分布情况评估客户整

体的网络质量，结果为差时将提供潜在问题分析建议。可以查看当前网络质量监测状态，近日网络质量，以及当前网络质量及网络诊断结果。

点击<质量定义>，用于设置检测网络实时质量定义设置。

统计网络质量的活跃用户少于N人数可以自定义填写。默认10人，允许输入1 - 100之间的数字。

全天质量查的定义：用于监测判断，当全天质量查的时间累积超过N分钟时，判断为网络质量差，默认30分钟，允许输入10 - 300之间的数字。

点击<选择日期>可以查看一周内的网络质量状态。

点击<监测对象>用来选择网络监测的网站。默认选择所有网站。用户也可以指定要监测的网站，最多可以有3个监测列表，每个列表最多100个域名。

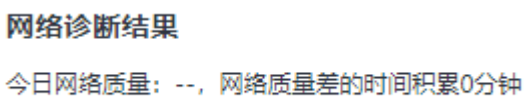
在检测对象下拉点击<管理>，进行编辑网站列表。

鼠标移到波形图上，出现悬浮框，可以看到详细的网络质量状态，当网络质量为差的时候，可以点击查看，进行查看上网慢用户列表。

纵坐标是统计到的在上网的用户个数，网络质量好的用户数+差的用户数。

鼠标移到波形图上，可以查看当前时间上网质量优和差的用户个数，点击<查看>可定位当前上网慢的用户列表。

网络诊断结果：用来查看详细的网络质量，可以显示若干条详细网络质量较差的原因。



可能存在的原因：

1. 未开启流控。
2. 带宽不足（如果当天存在连续10分钟http流量占带宽90%）。
3. P2P抢占带宽，建议限速，（如果当天连续10分钟p2p流量占带宽90%）。
4. 建议设置保证通道（流控有丢包10%以上且未设保证通道）。
5. 策略（xxx）流控限制较低。
6. 策略（xxx）连接数限制较低。

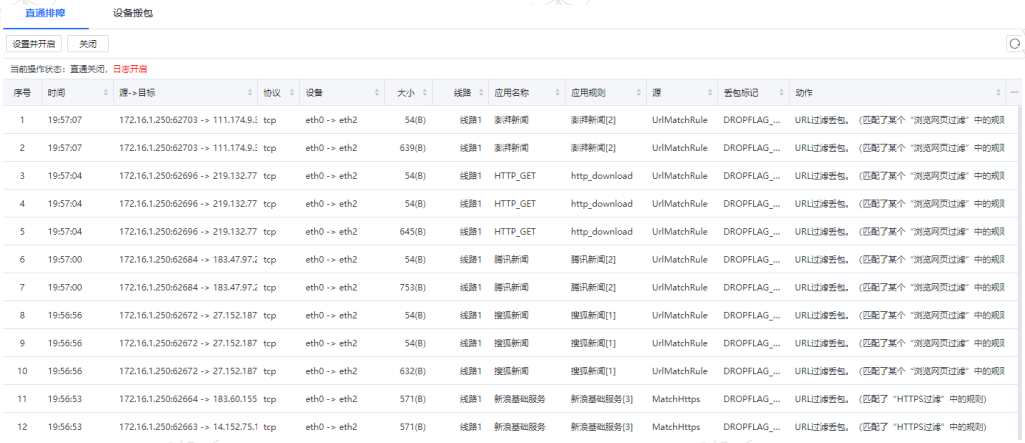
7. DNS配置错误。
8. 提示内侧或外侧性能瓶颈。

无法登录AC控制台

1. 检查设备面板上红色alarm灯是否常亮。
2. 是否能够正常ping通设备内网口。
3. 从内网是否能telnet通设备443端口。
4. Tracert设备内网口地址，查看数据包是否能够到达AC设备的管理口或者业务口地址。
5. 尝试用一台电脑通过交叉线接到DMZ口（缺省为ETH1口），将电脑的IP配成10.252.252.10/24，测试访问DMZ口的默认IP 10.252.252.252是否能通。
6. 如经过上述步骤仍无法登录设备，请联系深信服技术支持工程师。

网络应用无法使用

1. 检查网络应用本身是否正常。
2. 检查用户管理的上网策略，是否有设置可能拦截数据的策略。
3. 在上网故障排除模块下，将AC开直通再测试是否可以正常访问网络应用。
4. AC在网桥模式的部署下，开直通后，所有的上网策略不生效，AC起到连通网络的作用，开直通可以定位网络应用故障是否是由于AC上策略设置不当引起，如下图。



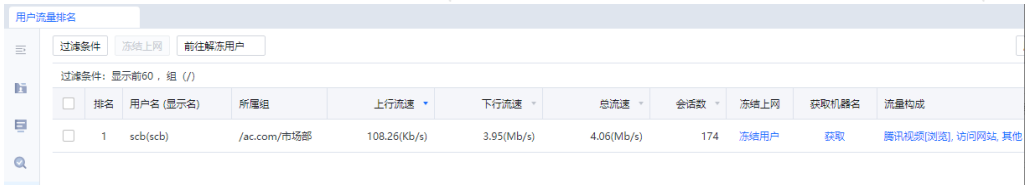
5. 上网故障排除功能开启后，会在列表中显示详细的拒绝日志，可根据拒绝日志排查是哪条策略拦截的数据，排错过程中建议指定IP地址开启日志，以便快速定位问题。
6. 尝试找一台上网不经过AC的电脑测试访问网络应用是否正常。
7. 如经过上述步骤应用依然无法正常使用，请速联系深信服技术支持工程师。

⚠ 注意：

问题定位后，请及时关闭用于上网故障排查的直通功能。

流控不生效

1. 在用户流量排名中检查指定用户的流量是否超过流量管理配置的阈值。



2. 检查网络是否有其他上网出口，当前用户上网是否未经过AC设备。

3. 检查设备当前是否开启了上网故障排除的直通功能。

4. 在[系统管理/系统设置]菜单栏禁用全局排除地址，检查是否因为全局排除导致流控策略不生效。

5. 检查针对当前用户是否有多条流控策略能够匹配，则用户的不同流量会匹配到多个通道，当前用户的流量相当于多个流量通道限制带宽的总和。

如下策略列表中，support用户会匹配[限制P2P下载]，该流控策略限制P2P下载等应用最大上行200Kbps，下行2Mbps。同时support用户还会匹配到[限制support用户流量],该流控策略限制support用户的所有流量上行200Kbps，下行2Mbps。则support用户在使用过程中理论最大可以流量可以达到上行400Kbps，下行4Mbps（P2P等应用上行200Kbps，下行2Mbps+其他所有应用上行200Kbps，下行2Mbps）。

6. 如经过上述步骤流控依然无效，请速联系深信服技术支持工程师。

经过AC上网比较慢

1. 开启上网策略故障排除的直通功能，测试上网是否正常
2. 在[全网监控/首页]查看当前设备运行状态，观察CPU占用是否长时间处于100%。
3. 在[全网监控/首页]查看当前应用流量排名，观察是否大量p2p下载等占用带宽。
4. 启用流量管理系统，限制p2p，下载，流媒体的带宽，保证上网及办公应用的带宽，测试打开网页是否正常。
5. 检查防DOS攻击日志，查看设备当前是否正遭受攻击。
6. 尝试找一台不经过AC上网的电脑，测试上网速度是否正常。
7. 如经过上述步骤网络依然异常，请速联系深信服技术支持工程师。

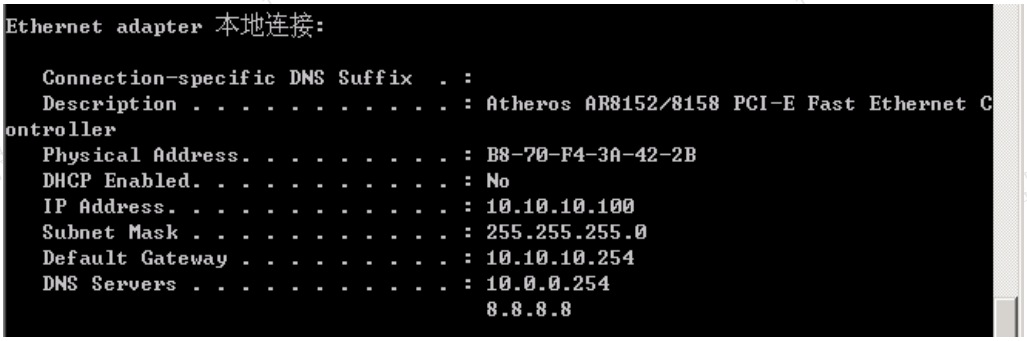
电脑弹不出认证页面

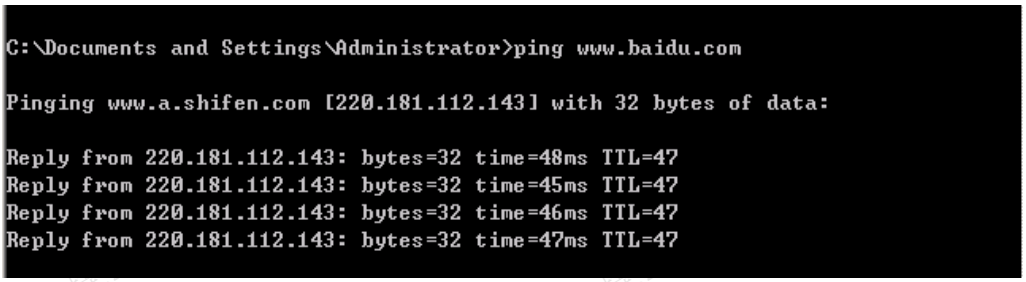
1. 检查AC设备认证策略是否启用密码认证，或者单点登录失败动作选择密码认证。

2. 检查AC设备到内网电脑的回包路由（网桥模式使用虚拟地址重定向不需要）。

3. 检查AC是否允许用户认证成功之前能访问DNS服务，以及使用HTTPS页面访问时开启重定向。

4. 客户端电脑检查网关和DNS设置是否正确，能否解析出域名。





⚠ 注意：

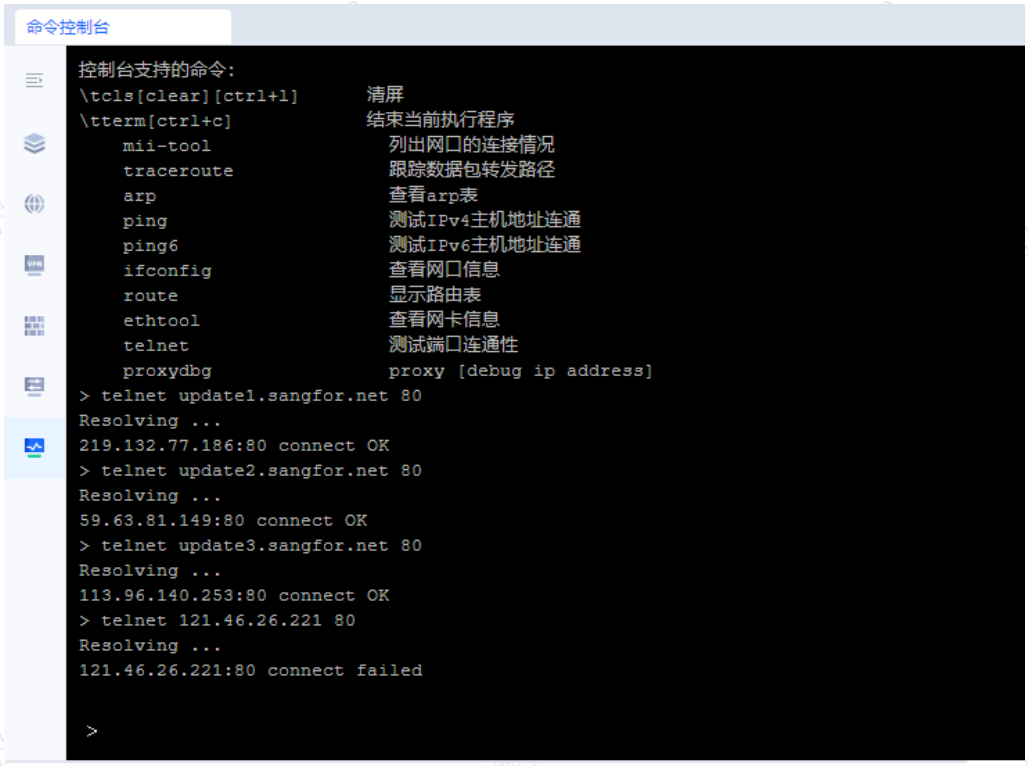
这里之所以能解析出域名并且能ping通外网地址,是因为在AC上启用了“未通过认证用户可以访问NDS服务”及“未通过认证用户具体根组权限（HTTP应用除外）”。

5. 重新访问外网测试用户认证框能否正常弹出。

6. 经过上述步骤，认证页面仍然无法打开，请联系深信服技术支持。

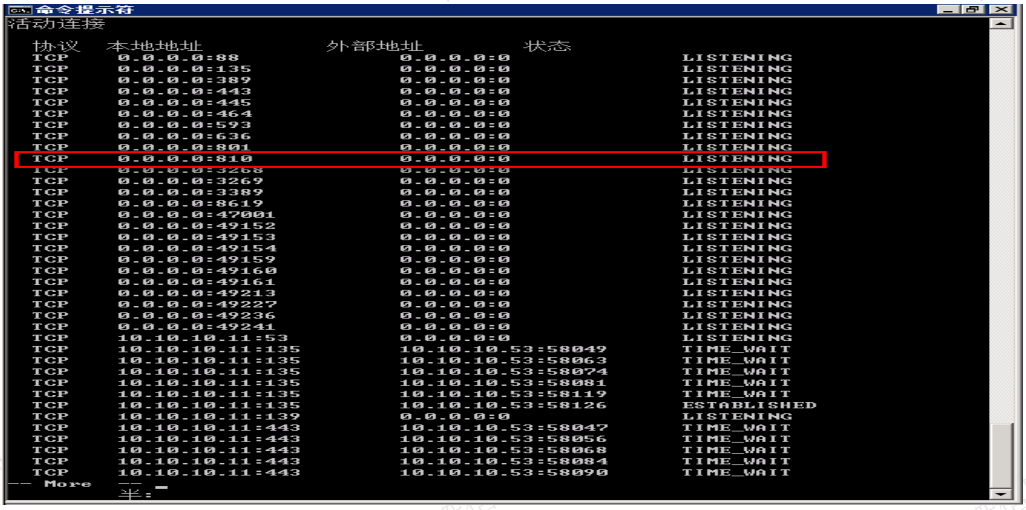
规则库无法更新

1. 检查[系统管理/系统配置/系统更新/规则库升级]中，相应规则库升级服务有效期是否显示“已过期”。
2. 通过命令控制台，检查设备本身到公网服务器连通性是否正常，即设备本身是否可以正常上网。
3. 通过命令控制台，检查设备与update1.sangfor.net、update2.sangfor.net、update3.sangfor.net、121.46.26.221这四个规则库更新地址的80端口通信是否正常。



日志中心无法同步

1. 登录外置日志中心,在[系统管理/系统状态/系统日志]下查看是否有错误以及告警日志。
2. 检查服务器本身810端口是否在正常监听。
3. 开始---->运行---->cmd，或者是window+R组合键，调出cmd命令窗口，输入命令， netstat -ano, 列出所有端口的情况。



4. 在AC命令控制台测试日志中心的TCP 810端口，检查AC设备到日志中心服务器之间是否有防火墙拦截了TCP 810端口。
5. 查看系统日志，通过系统日志可以检查：外置数据中心安装软件的版本和设备版本是否一致，外置数据中心同步账号和密码是否和设备上的一致。
6. 打开AC控制台，重新点击<同步>，检查是否可以正常同步。
7. 如经过上述步骤日志依然无法同步，请速联系深信服技术支持工程师。

突发事件应急处理

内网出现断网

1. 从内网PC上ping下AC设备，测试PC能否正常访问AC，如果能正常访问AC，尝试使用命令控制台从AC上分别ping一下网关和外网，确认外网是否正常。
2. 开启拦截日志并直通，看用户上网是否恢复，如果恢复，则通过查看拦截日志，找到拒绝数据的模块，修改策略。关闭拦截日志和直通，测试上网是否恢复正常，如果未恢复，则再开启拦截日志，根据拦截日志修改策略，直到故障修复。
3. 设备网桥部署时，确认设备桥接接口是否为bypass口，设备接口面板一般有标注bypass接口，如果未标注则默认ETH0和ETH2口是一对bypass接口，如果使用bypass接口为网桥接口，可尝试关闭设备测试。
4. 上述操作依然无法排除故障，可尝试跳过设备做进一步验证。
5. 如果跳过设备上网恢复正常，请联系深信服技术支持检查设备是否异常。
6. 如依然无法排除故障，请检查其他网络设备配置是否异常。

重要业务系统异常

1. 针对该业务系统，开启拦截日志并直通，看业务系统是否恢复正常，如果恢复，则通过查看拦截日志，找到拒绝数据的模块，修改策略。关闭拦截日志和直通，测试业务访问是否恢复正常，如果仍然未恢复，则再开启拦截日志，根据拦截日志修改策略，直到故障修复。
2. 设备网桥部署，确认设备桥接接口是否为bypass口，设备接口面板一般有标注bypass接口，如果未标注则默认ETH0和ETH2口是一对bypass接口，如果使用bypass接口为网桥接口，可尝试关闭设备测试。
3. 上述操作依然无法排除故障，可尝试跳过设备做进一步验证。
4. 如果跳过设备业务系统恢复正常，请联系深信服技术支持检查设备是否异常。

5. 如依然无法排除故障，请检查其他网络设备配置是否异常。

设备硬件故障

Alarm灯不亮，设备无法通电

1. 透明模式下跳开设备恢复网络，路由模式下直接联系技术支持。
2. 先确定设备有几个开关，部分设备只有一个硬开关，其他设备分为一个硬开关一个软开关，其中硬开关是设备外壳的开关，软开关是web界面中[系统管理/系统配置/系统诊断/重启操作]。
3. 如果只有一个硬开关的设备，打开开关，如果设备无法通电，Alarm灯不亮，更换排插和电源线，依旧无法通电，则联系深信服技术支持返修。
4. 如果设备有两个开关，则先打开硬开关，再按下软开关（弹性开关）方能正常开机。如果按上述方式操作后并且更换电源插座和电源线之后，设备仍不通电，则联系深信服技术支持返修。

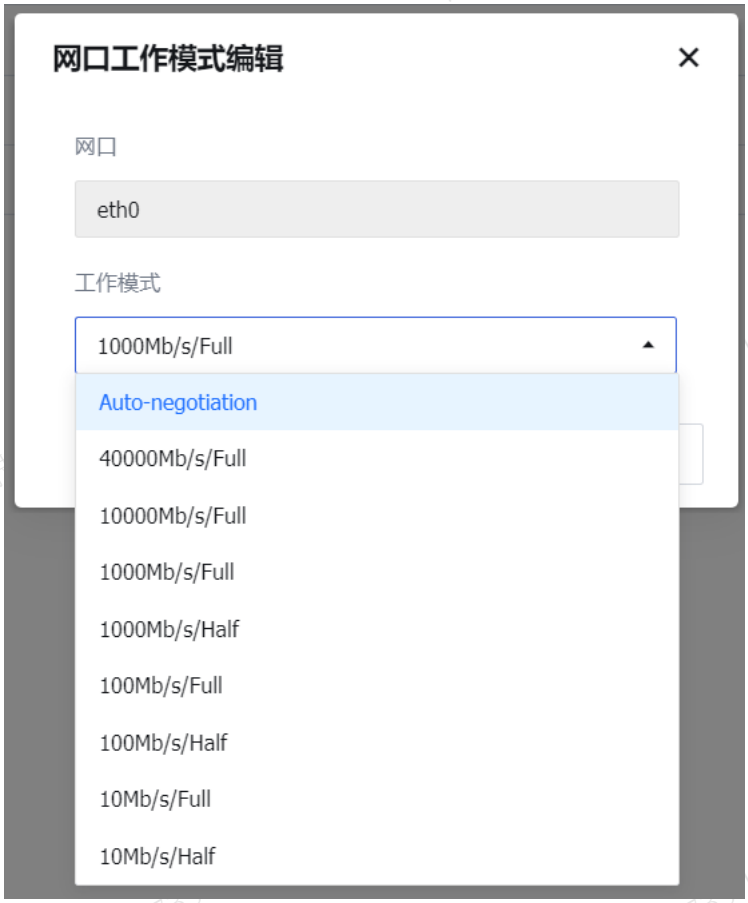
Alarm长亮，无法登录设备

1. 跳开设备恢复网络。
2. 关机30分钟后，再开机并等待2小时，如两小时内设备正常启动，说明设备之前进入自检状态，如两小时后alarm等依旧长亮，则联系深信服技术支持返修。

网口故障

1. 更换一根网线，检查接口能否正常工作。
2. 尝试修改故障接口的速率和双工模式，确认是否网口兼容性问题。
3. 在[系统管理/网络配置/网口配置]页面，点击接口当前的工作模式。

4. 分别尝试各种速率和双工模式，检查接口能否正常工作。



5. 将故障接口接交换机其他接口或其他网络设备，检查接口能否正常工作。
6. 将设备跳开网络，联系深信服技术支持确定硬件故障并返修。

缩略语

缩略语	英文全称	中文全称
SNMP	Simple Network Management Protocol	简单网络管理协议
RADIUS	Remote Authentication Dial In User Service	远程用户拨号认证服务
AP	Access Point	无线接入点
DNS	Domain Name System	域名系统（服务）协议
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
ARP	Address Resolution Protocol	地址解析协议
TCP	Transmission Control Protocol	传输控制协议
VLAN	Virtual Local Area Network	虚拟局域网

NAT	Network Address Translation	网络地址转换
BBC	Branch Bussiness Center	深信服集中管理平台BBC
IM	Instant Messaging	通讯软件
BA	Behavior Awareness	日志分析平台
EDR	Endpoint Detection and Response	终端检查响应平台
AD	Active Directory	活动目录
HA	High Availability	高可用性
MTU	Maximum Transmission Unit	最大传输单元
MSS	Maximum Segment Size	最大报文段长度
SAAS	Software as service	软件级服务
MAB	MAC Authentication Bypass	基于mac地址的IEEE 802.1x免认证