ACG1000应用控制网关基本功能介绍

H3C安全产品技术大练兵

引入

- 本课程在R6611版本基础上简述ACG1000应用控制网关常见的组网规划、常用的网络功能、用户认证技术、应用审计以及配合网管平台如何使用。便于大家在了解ACG1000设备基础功能前提下，进一步掌握一些功能实现原理以及基本的排错手段。

目录

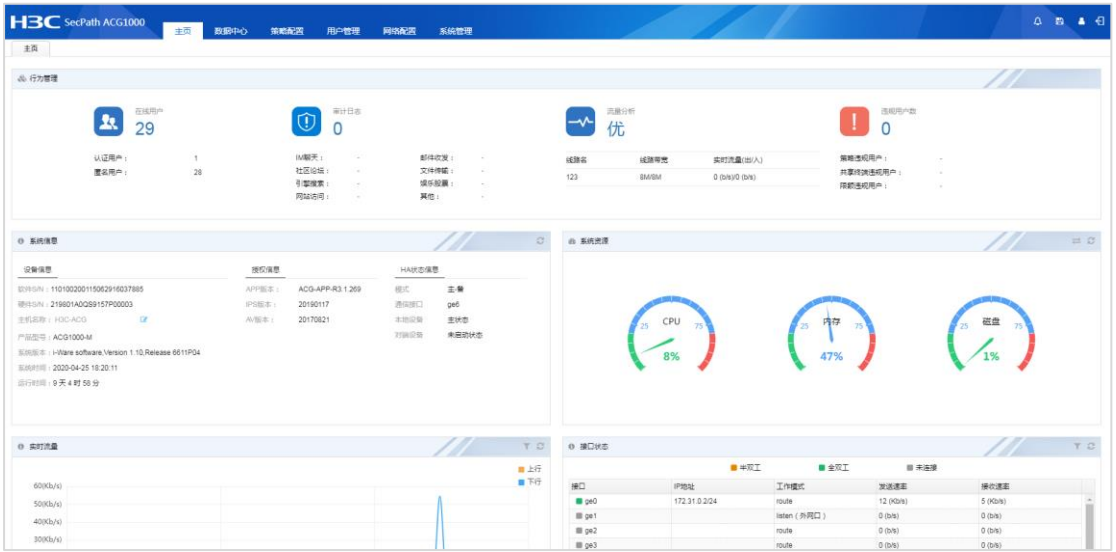
ACG1000两种不同版本分支

1 R6609P06版本（所有型号设备均能使用）

纵向导航栏，支持的功能没有新版本丰富。

用户名/密码：admin/admin

2 R6611P04（内存大于等于2G的型号才能使用）



导航栏全部横置，部分功能的配置逻辑发生变化

强制首次登录修改密码，密码必须包括数字，英文和字符，其中的字符包括!@#$%’,-.

- 可以通过查看规格表或者命令查看：H3C-ACG# display memory

注：R6609P06版本不能直接升级至R6611P04，需要先升级R6611，再从R6611升级至R6611P04

常用功能

R6609分支

- 适配所有版本的ACG manager

用户认证
应用审计
跨三层MAC学习
URL过滤
HTTPS解密
流量控制
无线非经
IPsec VPN
攻击防护
NAT
共享上网监控
链路负载

R6611P0X分支增加

- 不完全适配新老版本的ACG manager

入侵防御
SSL VPN
首次登录强制修改密码
访客二维码认证
病毒防护
弱密码防护
防暴力破解
DNS隧道传输检测
资产管理
风险扫描
策略梳理与分析
非法外联防护

ACG1000支持的授权

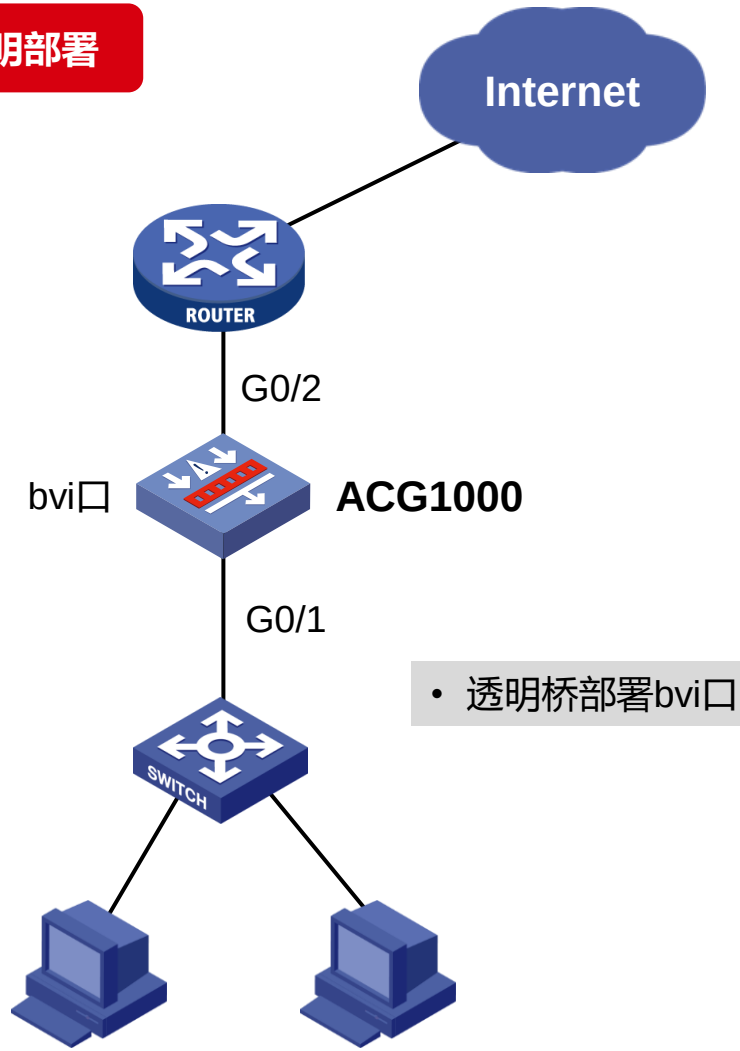
- R6609P06版本仅支持应用特征库和URL特征库升级的授权，但是R6611P04版本新增了功能，新增了IPS特征库以及病毒防护特征库升级授权以及非经SDK授权， web应用防护暂不需要授权。

Web应用防护缺省已经授权，SDK授权是通过任子行平台进行对接，而不直接和第三方进行非经对接。

目录

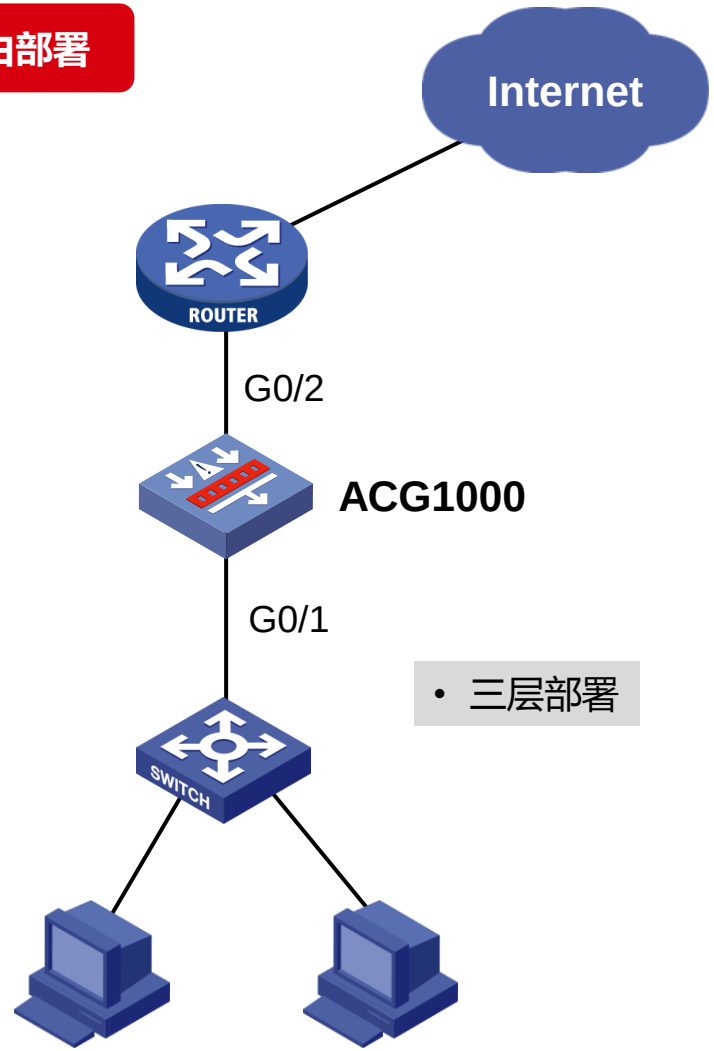
串行部署

透明部署



- 透明桥部署bvi口

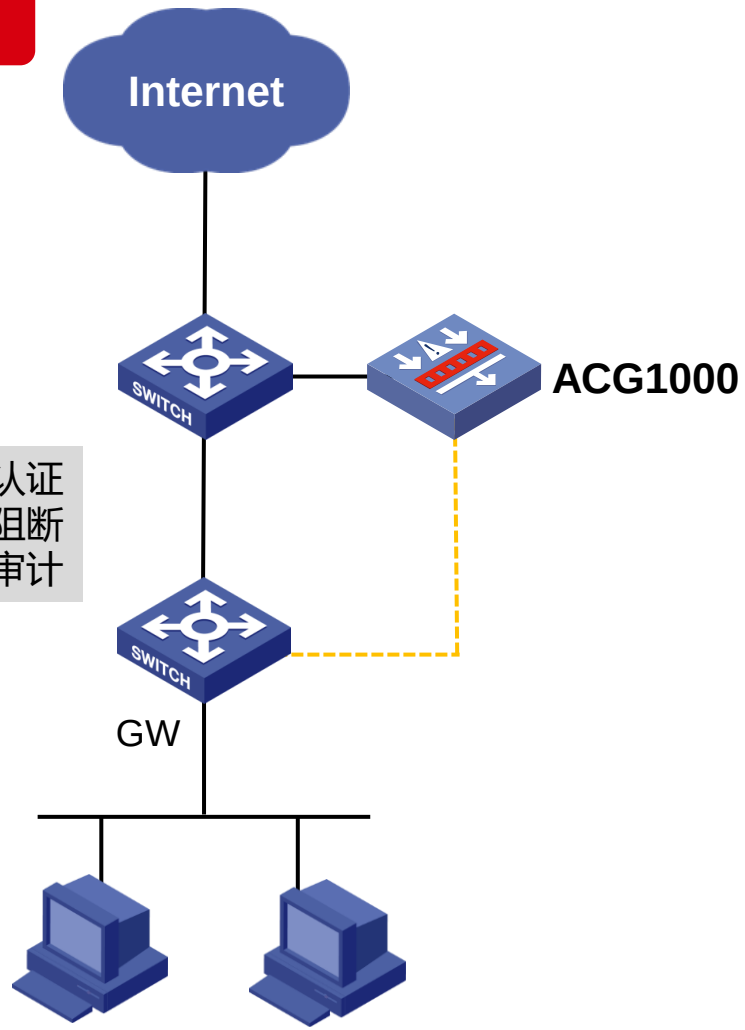
路由部署



- 三层部署

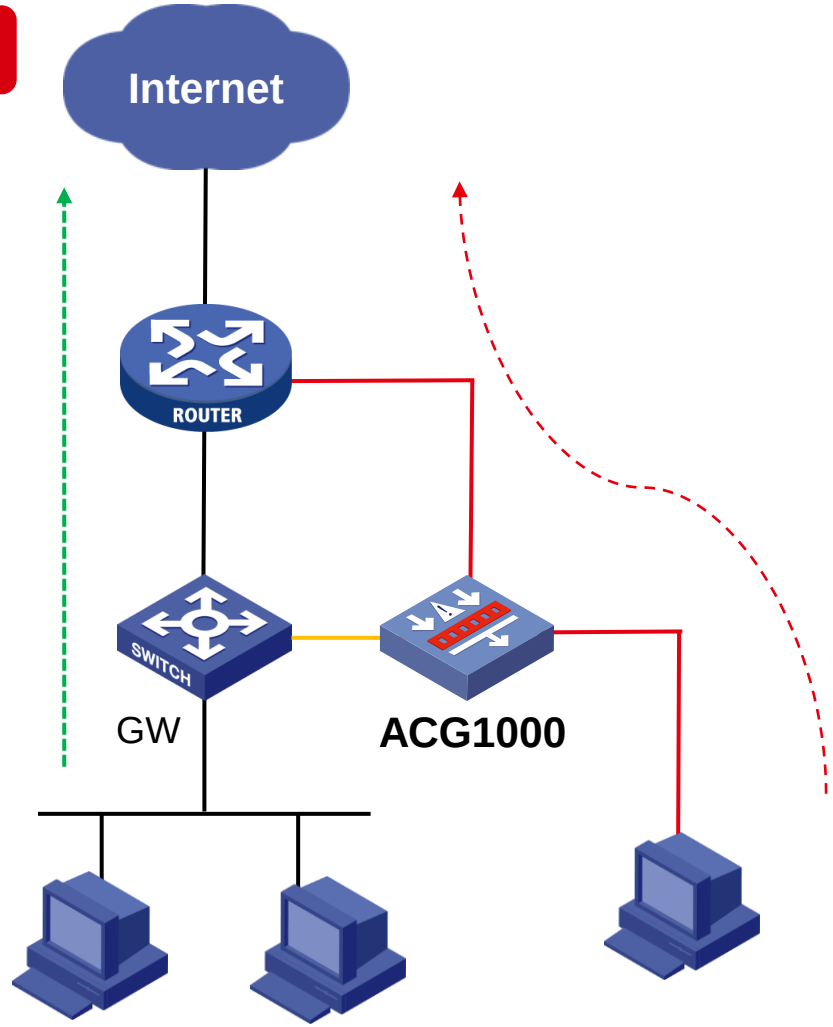
旁路部署

旁路镜像



- 旁路认证
- 旁路阻断
- 旁路审计

混合部署



双机部署

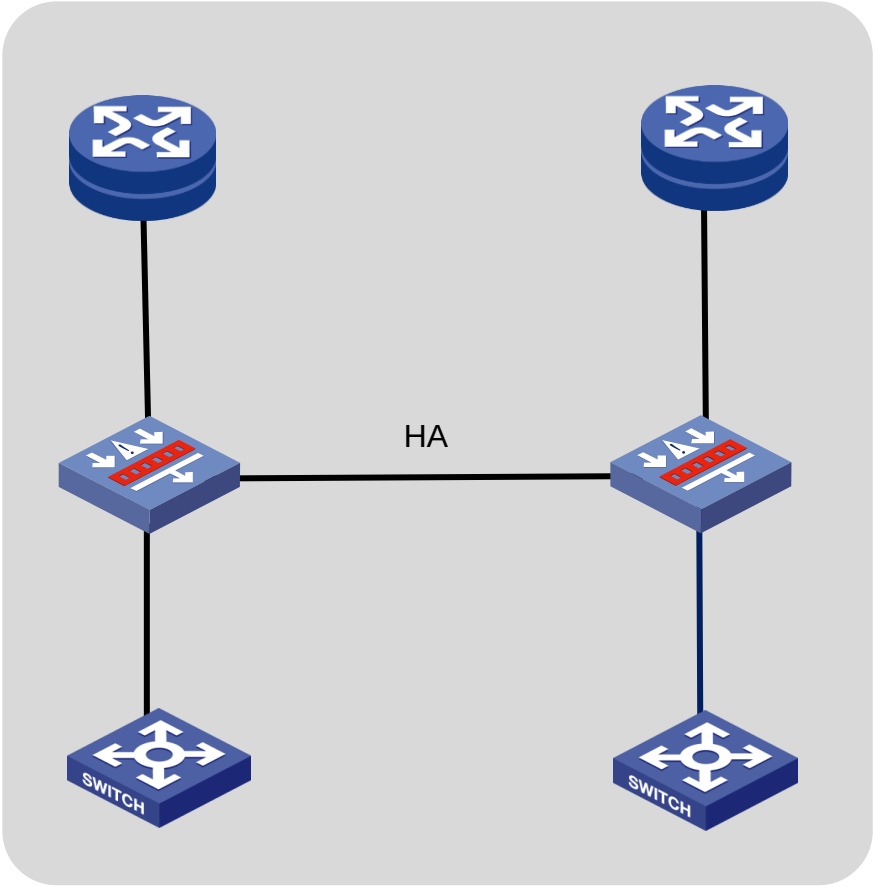
主备模式

- 主设备响应各类报文请求，并且转发网络流量；备用设备不响应报文请求，也不转发网络流量。主备设备之间通过HA心跳线同步状态信息，配置信息以及特征库文件。
- Session信息：包括设备连接表、FDB、用户信息、PKI。
- 设备配置：同步的设备配置中不包含HA配置信息，以及一些特殊的配置。
- 特征库：特征库包括APP特征库以及URL特征库。

主主模式

- 两台设备都配置成主动，使两台设备同时运行各自的工作，且相互监测对方的情况。当其中一台设备发生故障时，另外一台设备运行其自身的工作并且接管故障设备的工作，以保证整体业务不间断。兼具故障备份和负载均衡。HA主主模式下，同步内容有2种：运行状态同步、监控接口地址同步。
- Session信息：包括设备连接表、FDB、用户信息、PKI。
- 监控接口地址同步：当其中一台HA主主设备发生故障，那么另一台会代理这台故障设备的IP地址。

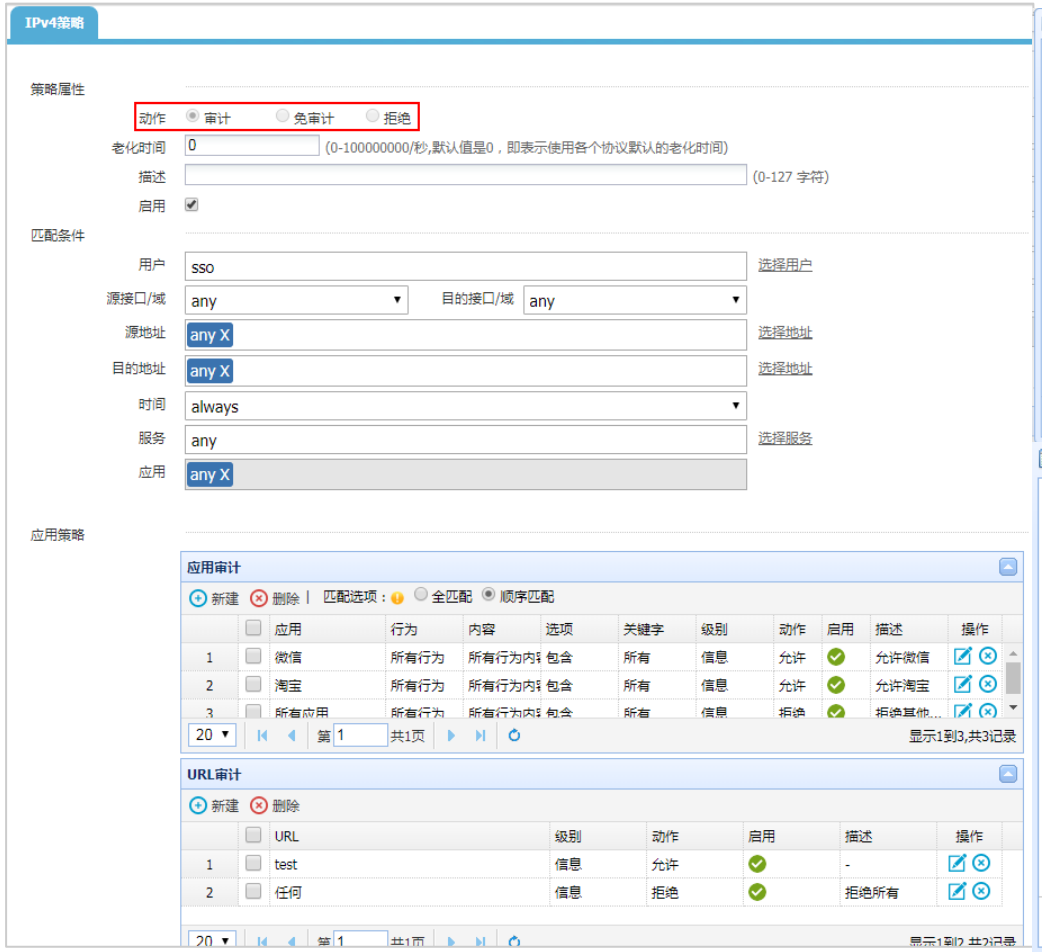
主备桥模式部署需要开启：
H3C-ACG(config)# ha-config
H3C-ACG(config-ha)# fdb refresh enable

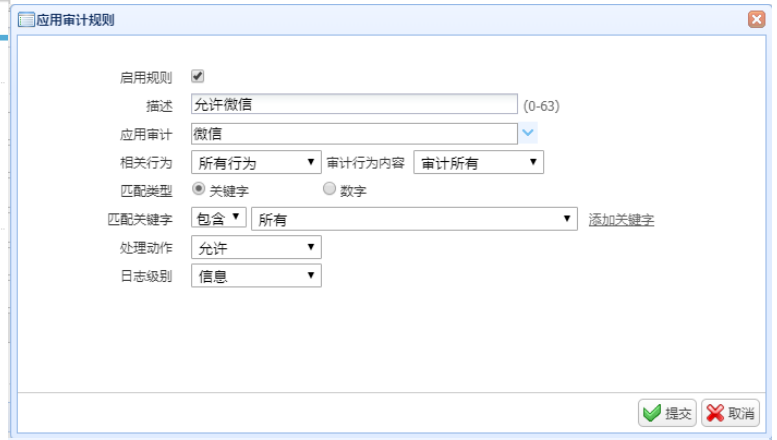


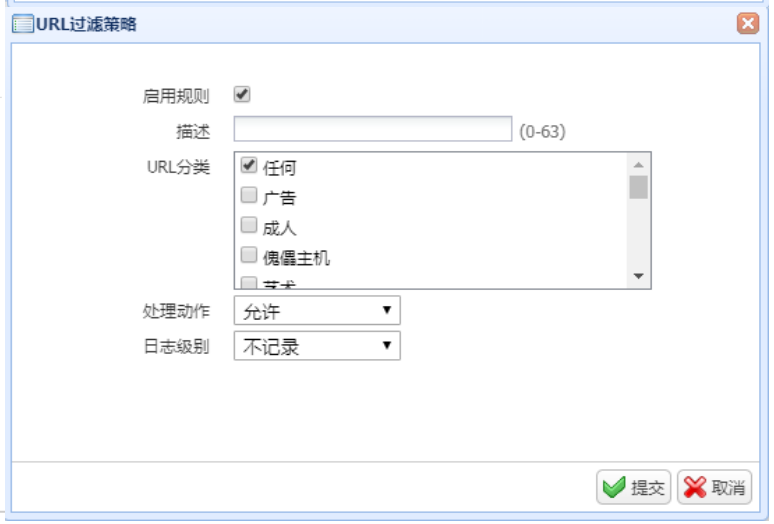
目录

IPv4应用控制策略（R6609分支）

- 应用控制和审计都是基于IPv4策略动作为审计的前提下，进入IPv4策略增加应用审计和URL审计策略。
- 应用审计策略缺省全匹配，可以手动修改成顺序匹配。URL过滤是全匹配，无法手动修改。

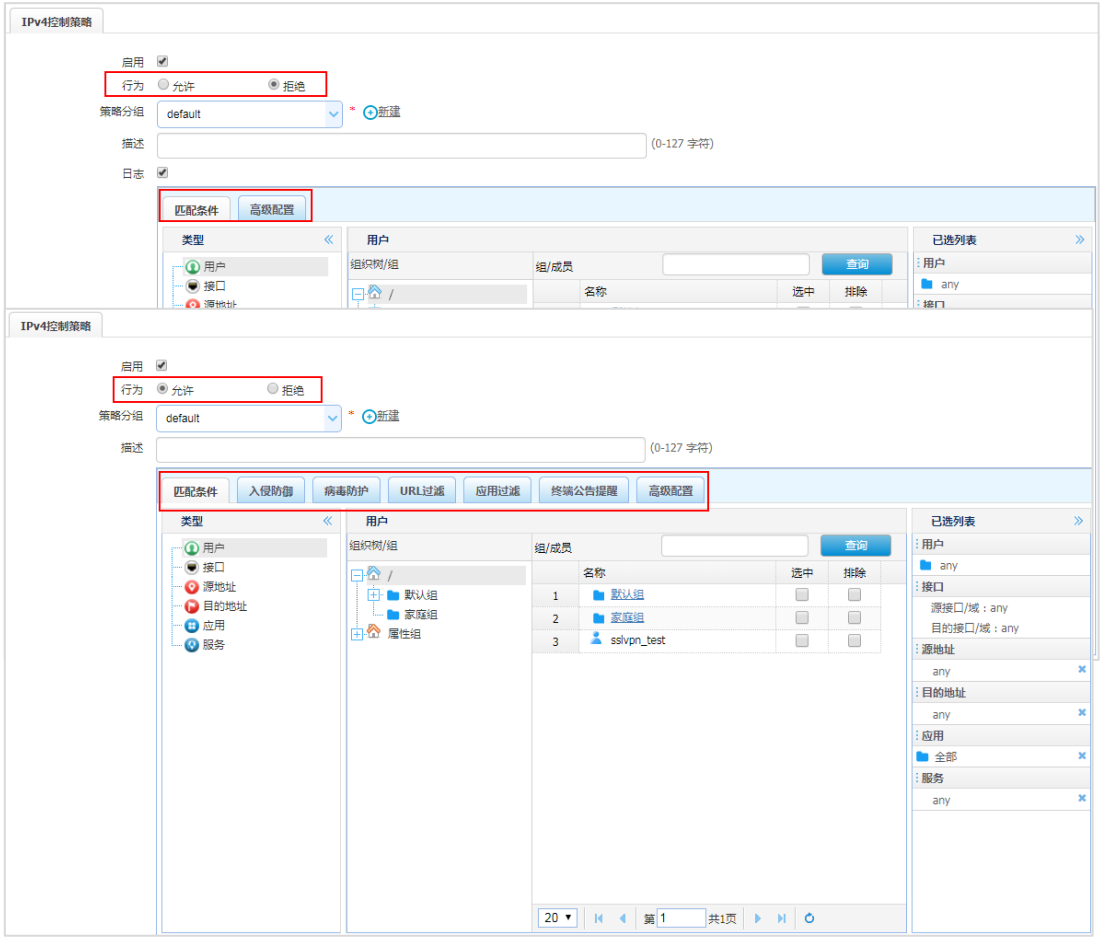






IPv4应用控制策略（R6611P0X）

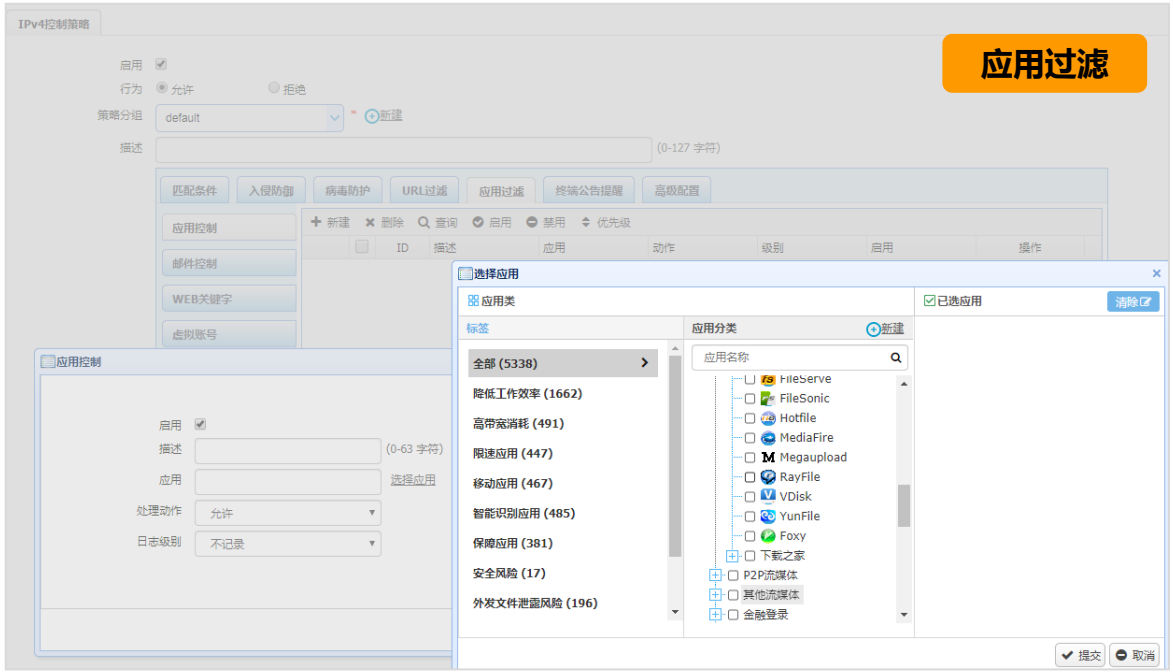
- 在新版本当中，将应用控制策略与应用审计策略拆分成了两个不同的配置选项。应用控制策略可以按照配置的的条件分别对不同的流量进行控制。
- 动作选为拒绝，那么流量就无法进行进一步检测，且生成的日志为流日志。（流日志必须发送给日志服务器才能识别）IPv4控制策略动作选允许，可以对流量进行IPS检测，防病毒检测、应用过滤等等，生成的日志为系统日志。



没有存储介质的ACG1000设备不支持查看审计、安全日志等。

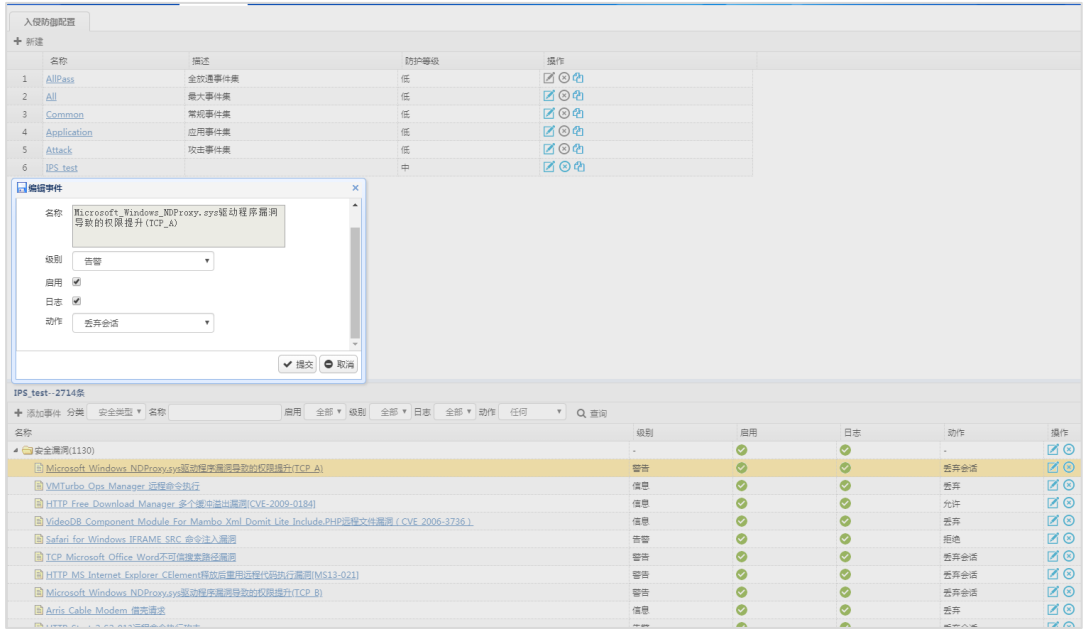
应用过滤和URL过滤

- 在R6611版本当中，可以选择不同的应用的动作进行过滤，日志在应用控制日志当中，也支持对WEB的关键字进行审计和过滤。



配置入侵防御

- 首先新增一个事件集，当然这个事件集也可以使用预置的事件集，但是预置的事件集无法对单条规则进行编辑。新增事件集之后点击添加事件，根据现网的需求选择需要防护的。



- 在IPv4控制策略当中调用入侵防御规则，可以选择事件集防御或者直接配置自定义的防护规则并启用自定义防御。

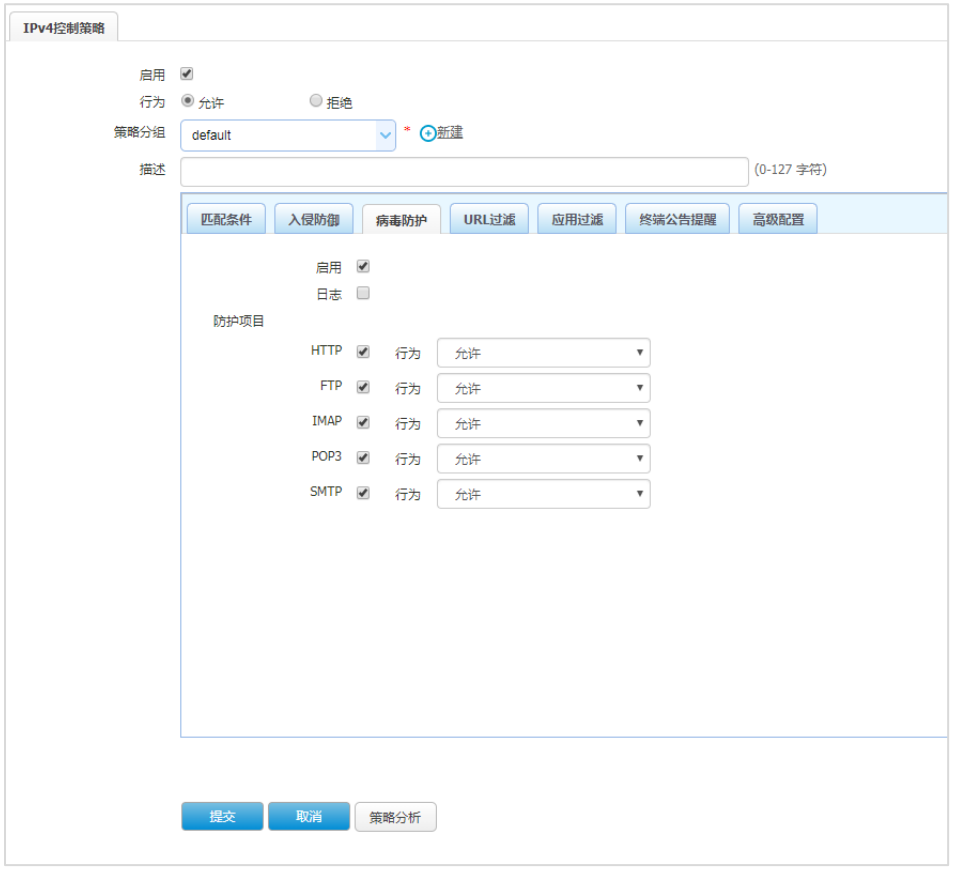
	时间	日志级别	用户名称	源地址	归属地	目的地址	事件名称	事件类型	行为	操作
1	2020-01-14 14:51:58	警告	101.3.13.12	101.3.13.12:57788	中国 台湾	183.1.1.35:80	zidingyiIPS	IPS自定义规则	允许	详细
2	2020-01-14 14:51:46	警告	101.3.13.12	101.3.13.12:57785	中国 台湾	183.1.1.32:80	zidingyiIPS	IPS自定义规则	允许	详细
3	2020-01-14 14:51:34	警告	101.1.41.22	101.1.41.22:55429	韩国	101.3.9.2:80	zidingyiIPS	IPS自定义规则	允许	详细
4	2020-01-14 14:51:32	警告	101.3.13.12	101.3.13.12:57784	中国 台湾	183.1.1.32:80	zidingyiIPS	IPS自定义规则	允许	详细
5	2020-01-14 14:51:28	警告	101.3.13.12	101.3.13.12:57783	中国 台湾	183.1.1.35:80	zidingyiIPS	IPS自定义规则	允许	详细
6	2020-01-14 14:51:25	警告	101.3.13.12	101.3.13.12:57783	中国 台湾	183.1.1.35:80	zidingyiIPS	IPS自定义规则	允许	详细
7	2020-01-14 14:51:15	警告	101.3.13.12	101.3.13.12:57782	中国 台湾	183.1.1.32:80	zidingyiIPS	IPS自定义规则	允许	详细
8	2020-01-14 14:51:15	警告	101.3.13.12	101.3.13.12:57782	中国 台湾	183.1.1.32:80	zidingyiIPS	IPS自定义规则	允许	详细

病毒防护

- 设备可以针对内外网入口处，进行实时的病毒扫描，将外来病毒隔离在内网之外，实现工作站被动防御病毒之外的主动病毒防护，我们可以在诸如HTTP、FTP、IMAP、POP3、SMTP等应用协议时进行文件扫描。

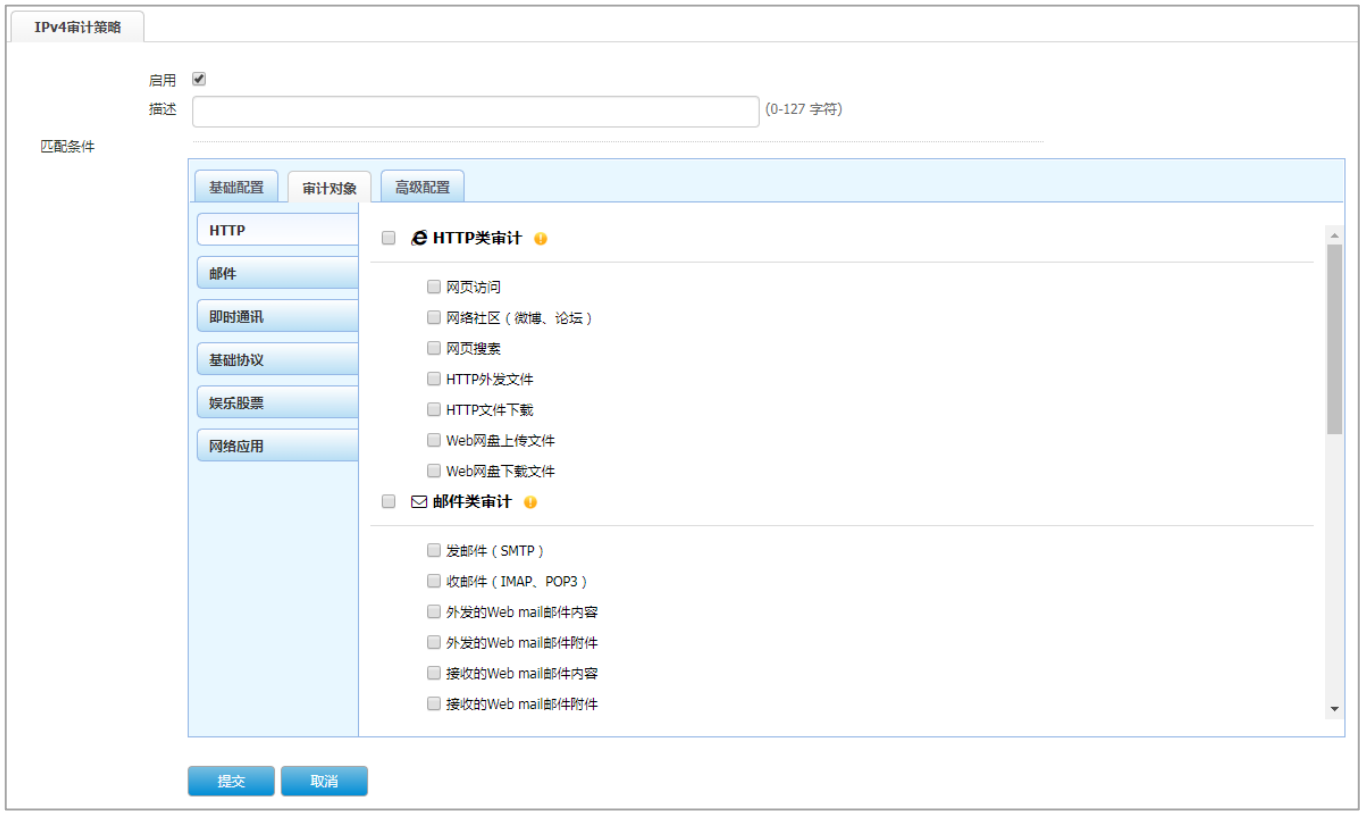
1 开启对压缩文件的检测

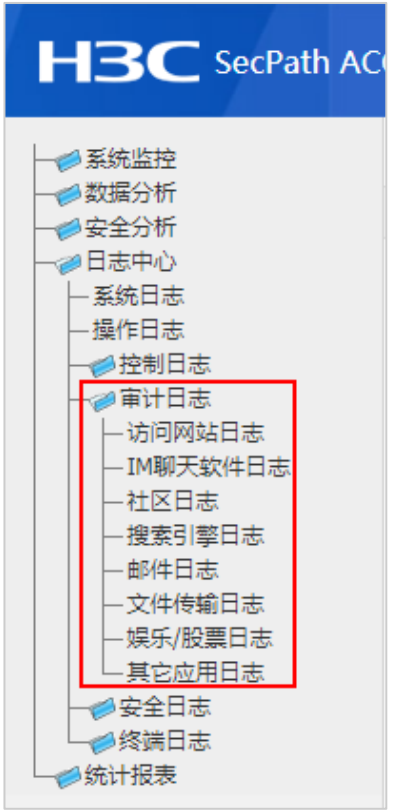
2 IPv4防护策略中开启“病毒防护”



IPv4审计策略

- IPv4审计策略是基于用户上网行为进行审计，审计从HTTP、邮件、即时通讯、基础协议、娱乐股票、网络应用等6大维度进行审计。





IPv4审计策略注意事项

1. 由于新版本控制和审计功能独立，不是识别出应用就记录日志的，需要审计到相关应用的账号或内容才会记录审计日志，由于有些是加密传输的，设备无法审计到相关内容，因此测试时需要配合解密的功能。
2. 不开启https解密，默认对内置的https网页进行审计，网页标题从内置的网站与标题的对应文件中获取。可以通过命令配置https audit all对所有https网页进行审计。
3. 网盘的上传下载需要开启HTTPS解密功能，网页版网盘上传、下载文件支持百度网盘、360网盘、网易网盘的审计；附件单个文件大小最大支持100M。
4. Webmail接收邮件只支持163、126、QQ邮箱三个，点击收邮件，且得点开邮件查看内容才会有收邮件的请求，才能审计到；如果要审计附件必须点击附件下载，才能审计到。加密邮箱必须要开启邮箱界面才能审计。
5. 即时通讯类能审计到登录账号信息和登录行为，无法审计内容。
6. 娱乐股票类审计目前必须审计到对应的账号或评论之后才能产生对应的审计日志；

详细介绍可以参考FAQ。

目录

用户分类

ACG1000有一个很重要的应用场景就是对不同的用户进行精细化地控制。所以前提就是能够精准地识别到用户，只有流量被识别成用户之后，认证、应用控制等功能才会生效。

默认情况下，未经过认证或是同步的流量，经过ACG的时候，且这些流量均在识别范围内，都会被识别成匿名用户

匿名用户

经过ACG1000认证或者其他第三方认证成功上线的用户。

认证用户

静态绑定用户

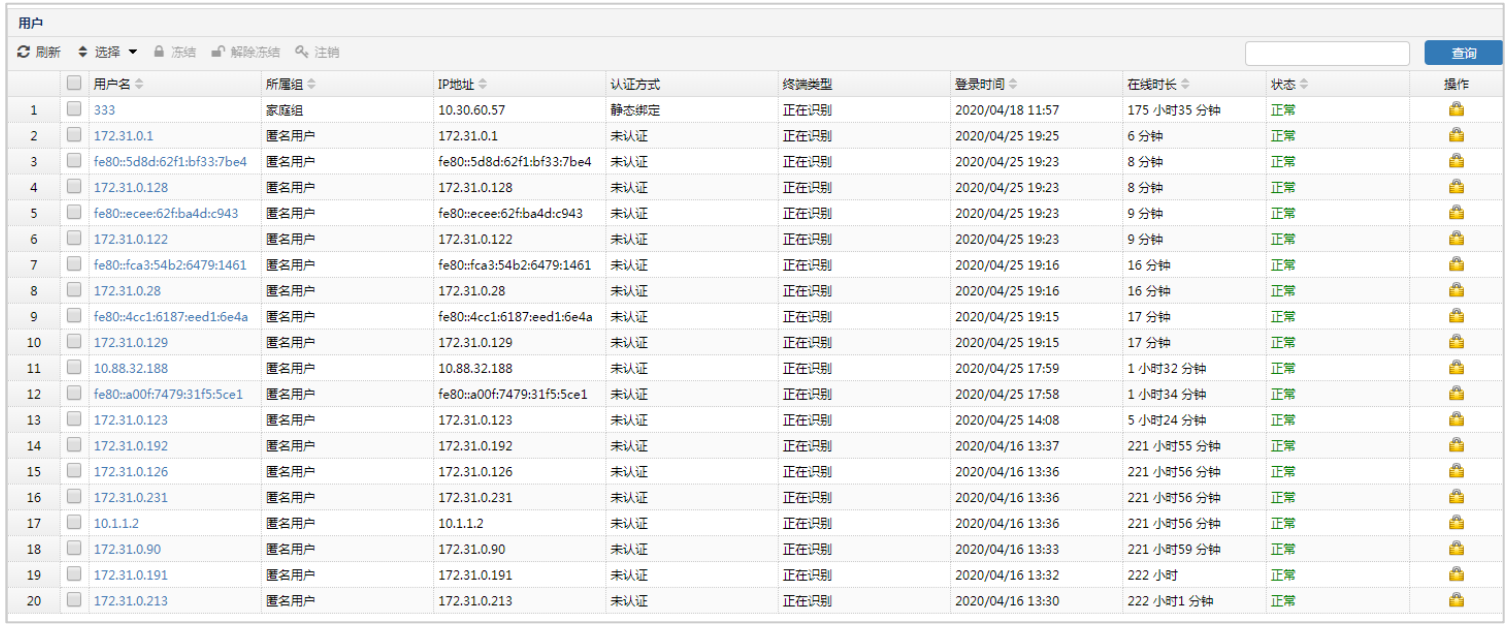
当用户的网络环境中使用的全部是固定地址时，可以在本地把用户和IP地址进行绑定

同步用户

从第三方同步过来的用户，LDAP同步、SNMP同步和ARP扫描。

匿名用户

- 默认情况下，ACG1000设备对于未经过认证的用户，以源IP地址作为元素进行用户识别，相关审计日志的用户都是用户的源IP地址。在实际环境中，经常会有一些公网地址或非用户源网段的IP被识别为匿名用户，此时可使用识别范围进行配置，只有属于引用地址对象内的源地址才会被识别为用户



	用户名	所属组	IP地址	认证方式	终端类型	登录时间	在线时长	状态	操作
1	333	家庭组	10.30.60.57	静态绑定	正在识别	2020/04/18 11:57	175 小时35 分钟	正常	
2	172.31.0.1	匿名用户	172.31.0.1	未认证	正在识别	2020/04/25 19:25	6 分钟	正常	
3	fe80::5d8d:62f1:bf33:7be4	匿名用户	fe80::5d8d:62f1:bf33:7be4	未认证	正在识别	2020/04/25 19:23	8 分钟	正常	
4	172.31.0.128	匿名用户	172.31.0.128	未认证	正在识别	2020/04/25 19:23	8 分钟	正常	
5	fe80::ecee:62f:ba4d:c943	匿名用户	fe80::ecee:62f:ba4d:c943	未认证	正在识别	2020/04/25 19:23	9 分钟	正常	
6	172.31.0.122	匿名用户	172.31.0.122	未认证	正在识别	2020/04/25 19:23	9 分钟	正常	
7	fe80::fca3:54b2:6479:1461	匿名用户	fe80::fca3:54b2:6479:1461	未认证	正在识别	2020/04/25 19:16	16 分钟	正常	
8	172.31.0.28	匿名用户	172.31.0.28	未认证	正在识别	2020/04/25 19:16	16 分钟	正常	
9	fe80::4cc1:6187:eed1:6e4a	匿名用户	fe80::4cc1:6187:eed1:6e4a	未认证	正在识别	2020/04/25 19:15	17 分钟	正常	
10	172.31.0.129	匿名用户	172.31.0.129	未认证	正在识别	2020/04/25 19:15	17 分钟	正常	
11	10.88.32.188	匿名用户	10.88.32.188	未认证	正在识别	2020/04/25 17:59	1 小时32 分钟	正常	
12	fe80::a00f:7479:31f5:5ce1	匿名用户	fe80::a00f:7479:31f5:5ce1	未认证	正在识别	2020/04/25 17:58	1 小时34 分钟	正常	
13	172.31.0.123	匿名用户	172.31.0.123	未认证	正在识别	2020/04/25 14:08	5 小时24 分钟	正常	
14	172.31.0.192	匿名用户	172.31.0.192	未认证	正在识别	2020/04/16 13:37	221 小时55 分钟	正常	
15	172.31.0.126	匿名用户	172.31.0.126	未认证	正在识别	2020/04/16 13:36	221 小时56 分钟	正常	
16	172.31.0.231	匿名用户	172.31.0.231	未认证	正在识别	2020/04/16 13:36	221 小时56 分钟	正常	
17	10.1.1.2	匿名用户	10.1.1.2	未认证	正在识别	2020/04/16 13:36	221 小时56 分钟	正常	
18	172.31.0.90	匿名用户	172.31.0.90	未认证	正在识别	2020/04/16 13:33	221 小时59 分钟	正常	
19	172.31.0.191	匿名用户	172.31.0.191	未认证	正在识别	2020/04/16 13:32	222 小时	正常	
20	172.31.0.213	匿名用户	172.31.0.213	未认证	正在识别	2020/04/16 13:30	222 小时1 分钟	正常	

强制模式：仅会话源地址在地址对象内的IP地址被识别为用户，其他一律不识别为用户；

启发模式：在配置了一个地址对象以后，按照以下：

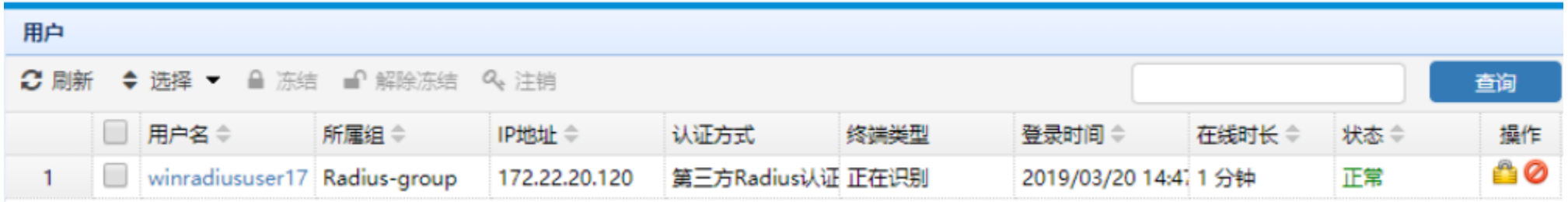
- → 会话的源地址和目的地址均不在地址对象范围内，将会话的发起方地址作为用户；
- → 会话的源地址和目的地址其中一个在地址对象范围内，取在范围内的地址作为用户；
- → 会话的源地址和目的地址均在地址对象范围内，将会话的发起方地址作为用户；

认证用户

- 认证用户主要是指通过ACG1000设备上支持的认证功能上线之后的用户。主要包括本地web认证、短信认证、第三方服务器（LDAP、RADIUS）、单点登录以及新版本支持的访客二维码认证。
- 以上这些用户上线之后会按照配置被识别成功对应的用户和用户组，ACG1000可以针对这些用户组进行应用上的权限控制、流控和审计等行为。

配合服务器认证用户

ACG产品可配合radius服务器和LDAP服务器进行认证，全局进行开启之后，正常配置本地web认证。



同步用户

同步用户可以分为本地同步用户（LDAP同步、SNMP同步、ARP扫描）以及第三方用户用户同步。

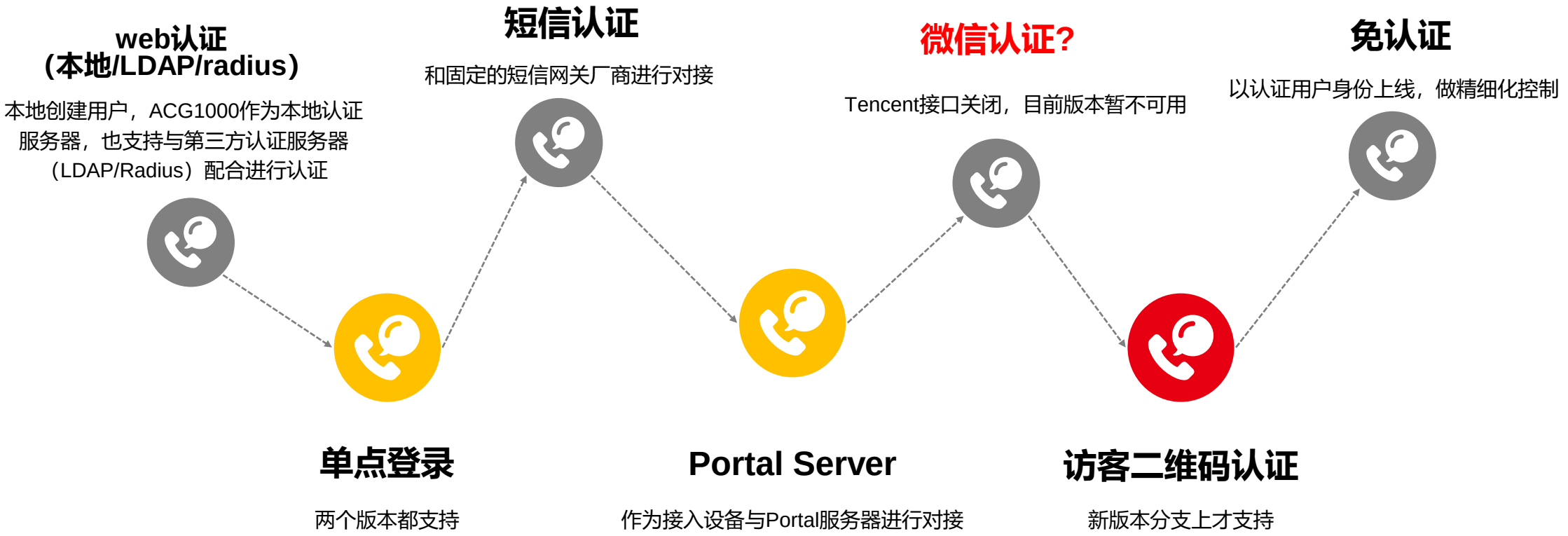
本地同步同步：LDAP同步、SNMP同步（跨三层MAC学习）、
ARP扫描（同网段）

第三方同步：

- 第三方同步用户接口：通过UDP9999端口接收用户上下线报文
- Radius用户同步：通过经过设备的Radius报文来识别用户。
- Web用户同步：通过经过设备的http认证报文来识别用户。
- 其他用户同步（特定的平台：深澜、城市热点等）

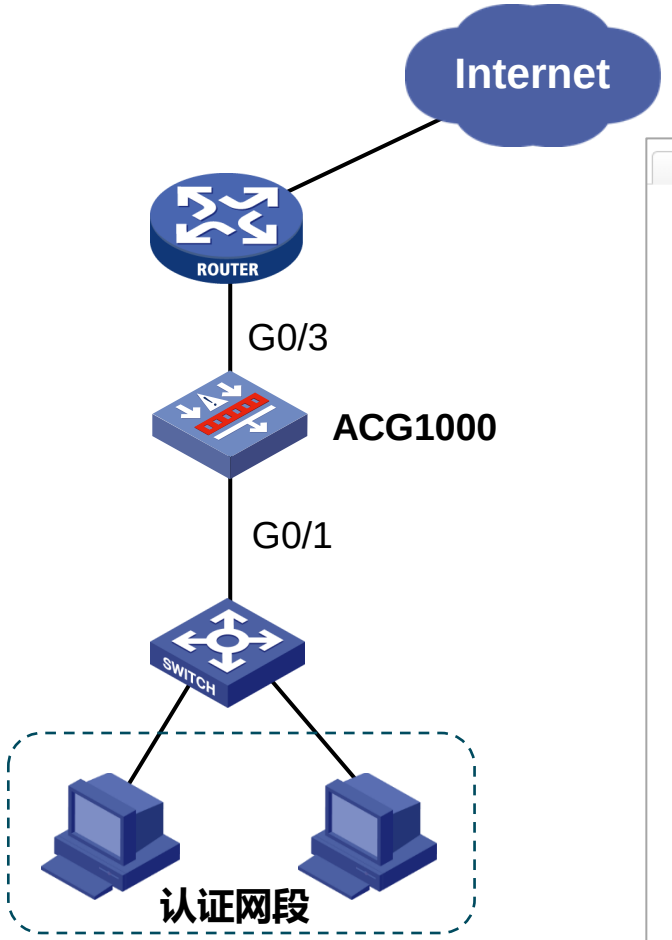
用户认证

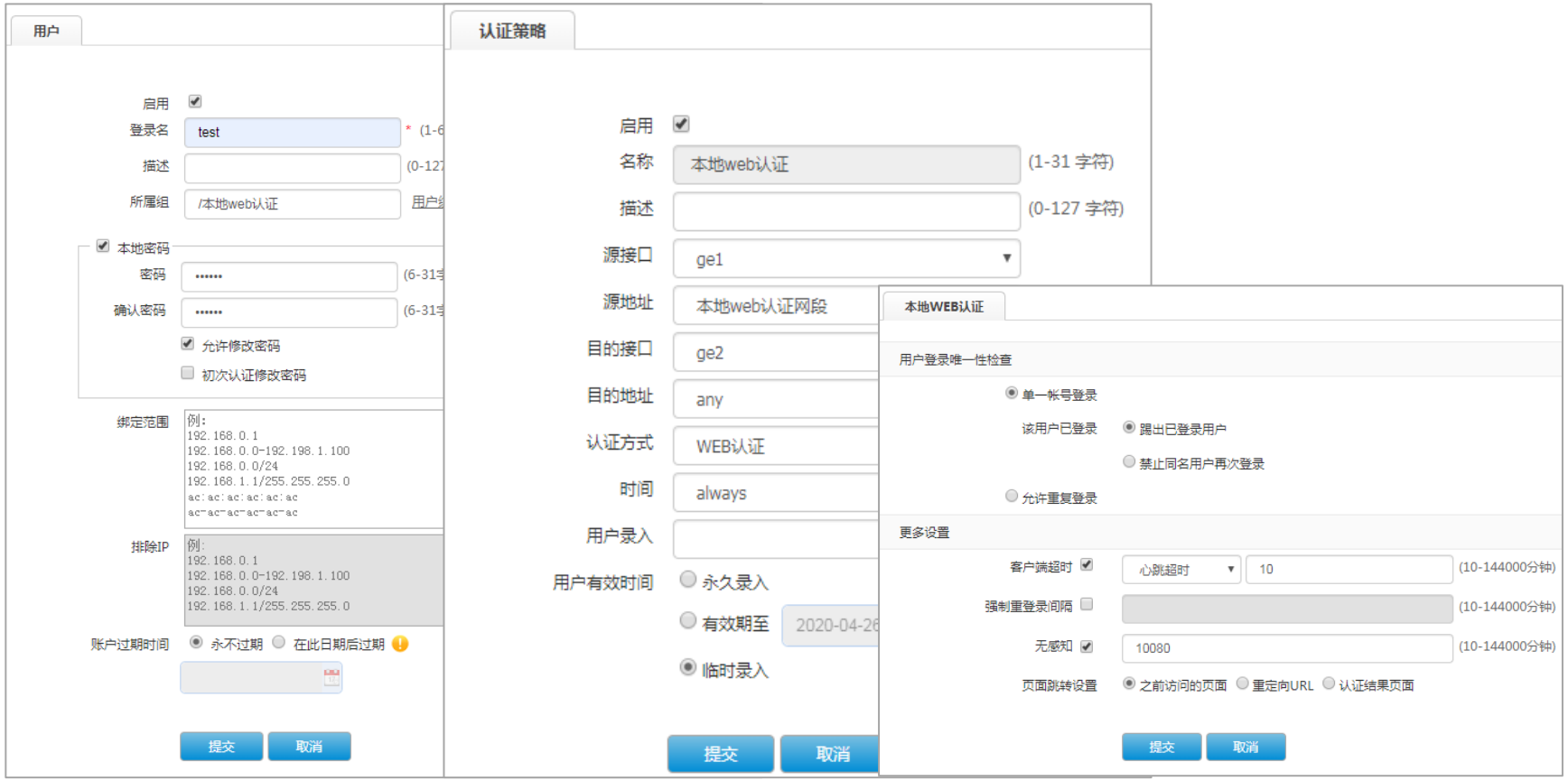
- ACG1000产品常用的一种情景就是在链路当中进行访问控制，只有通过认证的终端才能访问外网，或者控制部分终端必须要进行认证，其他终端可以正常访问外网。



本地web认证

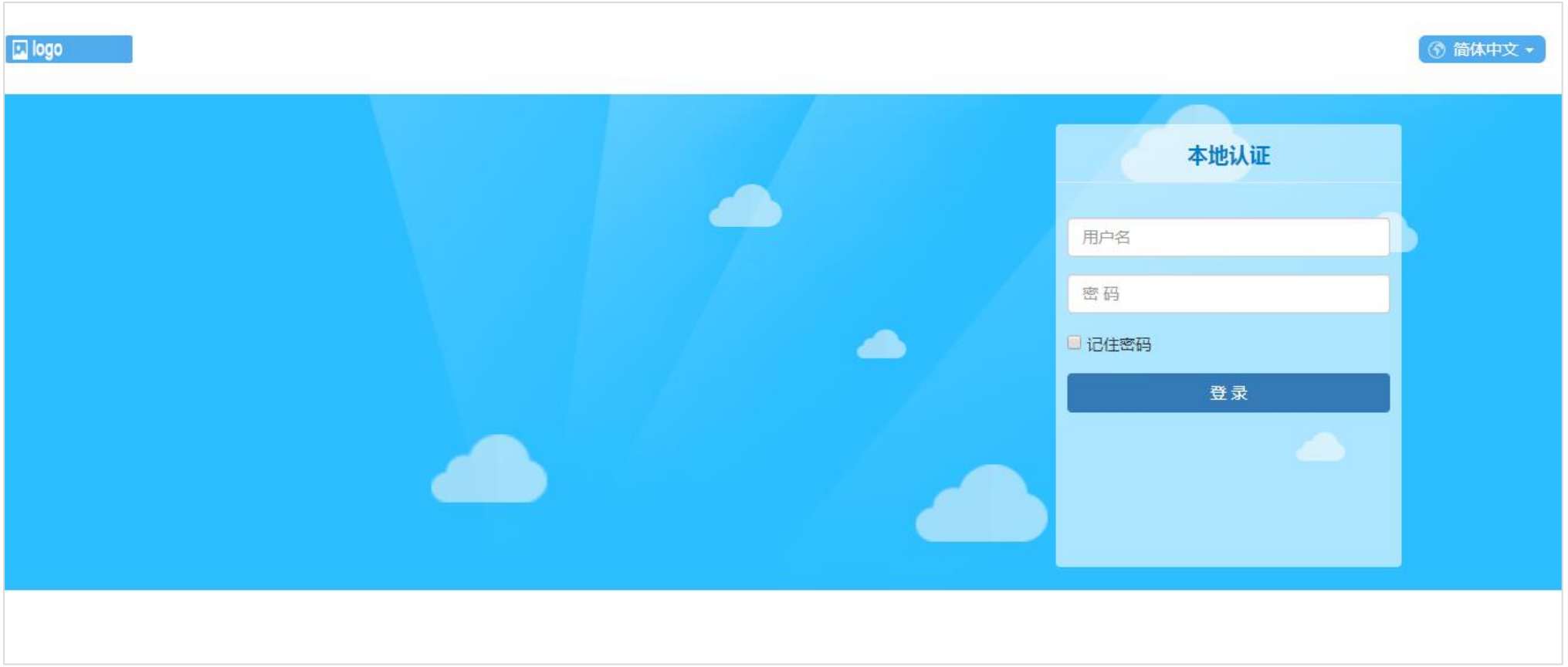
目前见过最常见的认证方式就是本地web认证。在ACG1000本地创建或者手工导入用户之后，内网用户只有通过认证才能访问外网资源。





本地web认证

内网用户在打开HTTP或者HTTPS（需要手动开启命令）网页的时候直接弹出认证的portal页面。



访客二维码认证（R6611P04版本支持）

访客二维码认证应用场景：

- 对于企业访客，联网之后终端弹出认证二维码，由公司内部审核人员（比如前台），扫描二维码，备注访客信息，然后实现访客上网；
- 对于酒店客户，手机可以通过微信认证上网，而笔记本无法进行微信认证，可以选择二维码认证，客户通过已经认证的手机，扫描笔记本二维码完成认证，最终实现笔记本上网。这种方式下，不需要弹出审核页面，直接以审核人身份上网。

1 访客二维码认证

2 配置访客二维码的认证策略

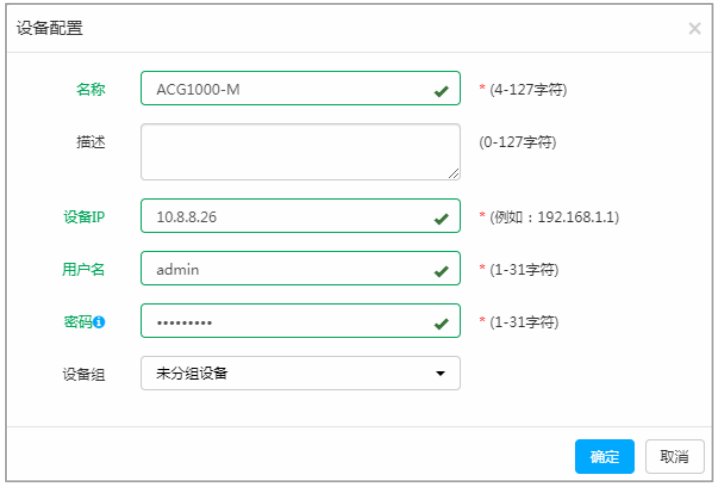
访客二维码认证（R6611P04版本支持）

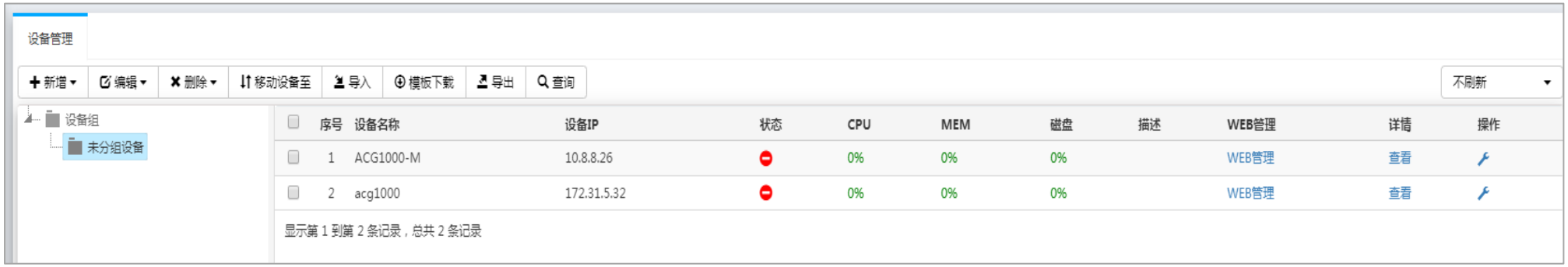
访客连上网络之后会弹出认证二维码的portal页面，要求必须是已认证用户（也就是审核员）扫描二维码输入访客的名字，登录成功之后访客才能正常上线。

目录

设备添加

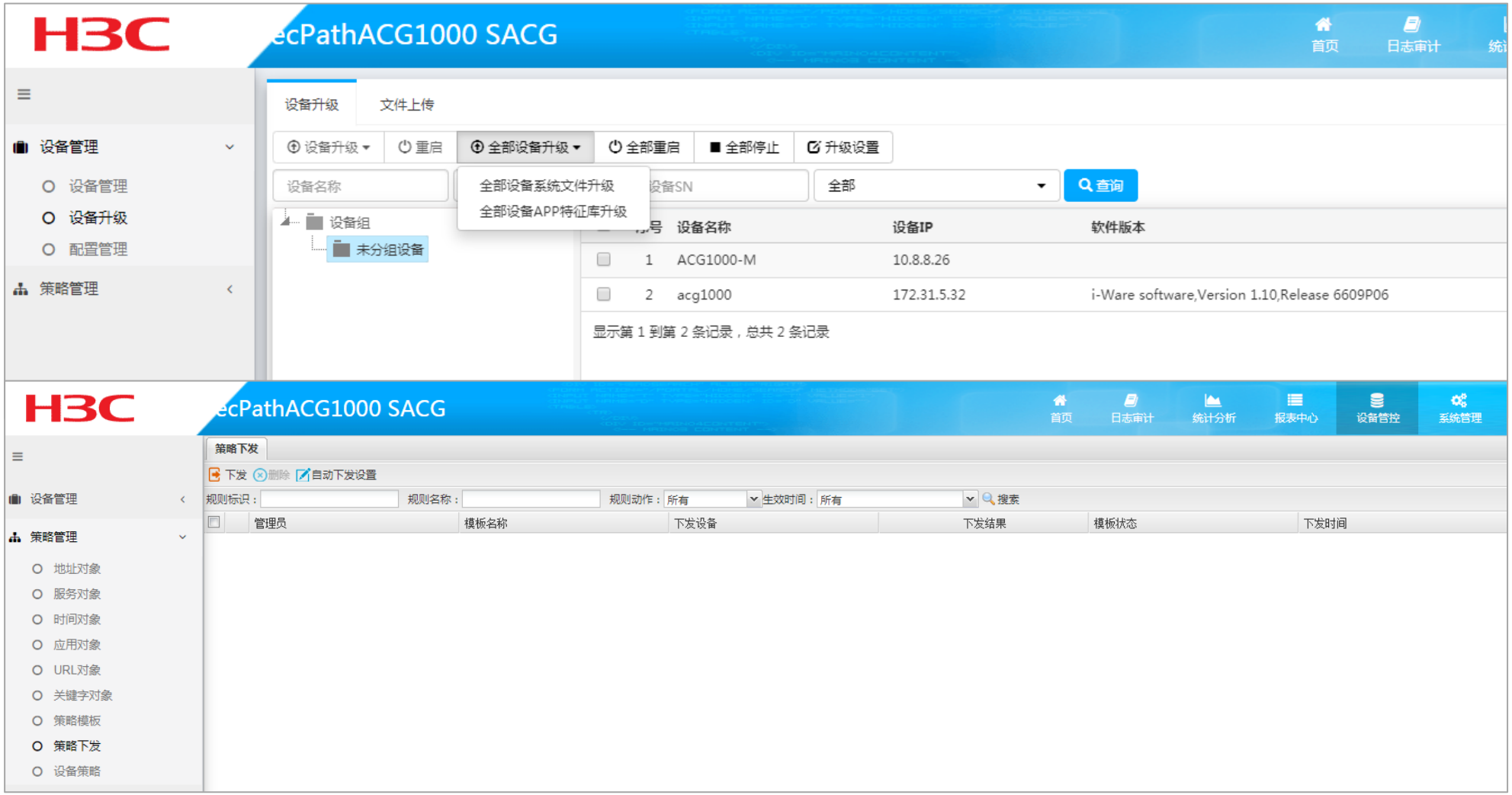
ACG日志分析与管理平台以设备或设备组为单位进行工作，配置时首先添加设备或设备组。添加时支持使用excel表格导入，使用IP地址+用户名+密码的条件添加设备





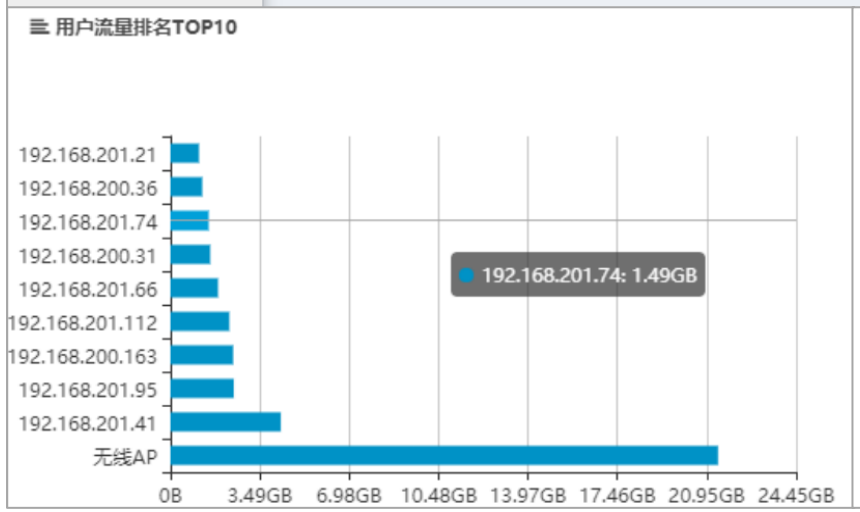
设备管理

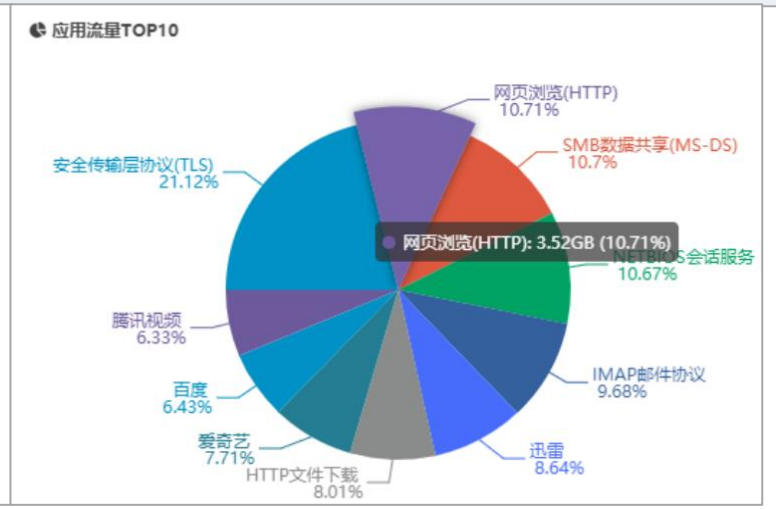
ACG日志分析与管理平台可在本设备上保存系统版本和特征库，并对已加入的在线设备进行统一升级。升级特征库后无需重启，升级主软件版本后可远程手工重启设备。还可以对设备进行批量的配置备份和策略下发。



日志的统一收集与分析

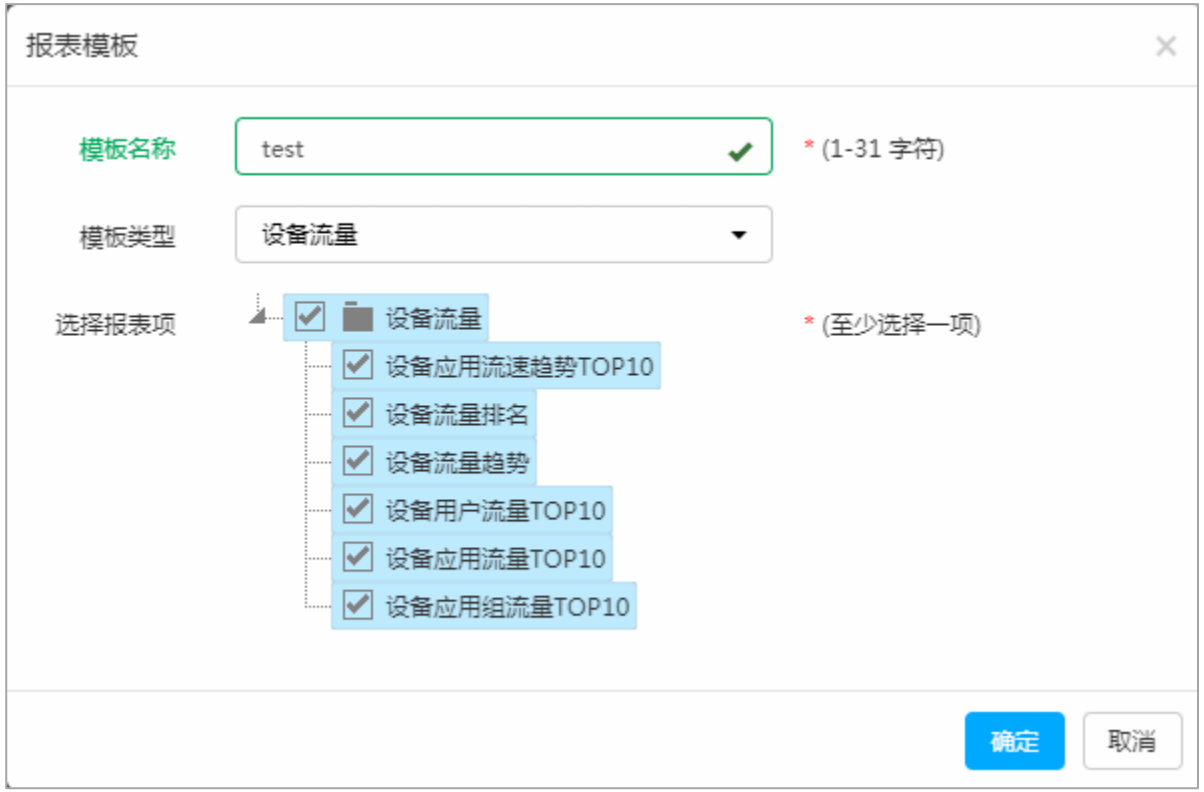
ACG日志分析与管理平台添加设备后，设备把日志日志分析与管理平台实时收集设备日志，进行统一的存储和维护，并支持自定义搜索字段来查询日志，方便用户按条件查看各类日志信息。同时，日志分析与管理平台对收集的日志进行统计分析，生成可视化的统计图表，为网络和设备的统计分析提供参考依据。





报表导出

日志分析与管理平台可根据所收集的日志数据，按照一定的时间周期生成报表文件，并通过邮件发送给相关人员。通过报表中心用户可以定制感兴趣的报表类型。系统支持 3 种报表类型，包括上网行为、设备流量、设备状态，这些报表的生成是基于对接收到的日志进行的分析。用户在配置报表模板后，新建报表任务，可以选择将报表发送到自己的邮箱，也可以生成报表后通过网页下载。



日志分析与管理平台授权

- ACG1000日志分析与管理平台在安装完成后默认有90天的试用期，试用期内可以纳管3000台以内数量的设备（包含高端和低端）。90天试用期过后，只可以纳管9台低端设备；如果需要管理高端设备及更多数量，请购买对应授权即可。
- ACG1000日志分析与管理平台授权分为两种，分别为集中管理授权、高端型号管理授权：
- 集中管理授权激活后，ACG1000日志分析与管理平台最多可管理3000台型号为ACG1000-B、ACG1000-C、ACG1000-S、ACG1005、ACG1005-PWR、ACG1010、ACG1010-X1、ACG1020、ACG1030、ACG1030-X1、ACG1040、ACG1050、ACG1050-X1、ACG1000-AK110、ACG1000-AK120、ACG1000-AK130、ACG1000-AK140、ACG1000-AK150、ACG1000-SE、ACG1000-SE-PWR、ACG1000-BE、ACG1000-BE-PWR、ACG1000-AK210、ACG1000-AK220、ACG1000-AK230、ACG1000-AK240的设备。
- 高端型号管理授权激活后，ACG1000日志分析与管理平台可管理小于10台ACG1060、ACG1070、ACG1000-AK160/AK170/AK180、ACG1000-AK250/AK260/AK270/AK280、ACG1000-M/A/E/T/P/X、ACG1000-blade-E、ACG1000-blade-X、ACG1000-ME、ACG1000-TE、ACG1000-AE、ACG1000-EE、ACG1000-PE、ACG1000-XE1、ACG1060-X1和ACG1070-X1型号的设备。
- 集中管理以及高端型号管理授权全部激活后，ACG1000日志分析与管理平台则可管理3000台设备（含高端型号）。

目录

IPv4控制策略配置举例

现场要求：内网网段172.16.10.0/24要求仅允许访问www.test.com这个网站，不允许打开其他的网站。并且能记录相关的日志，查看这个网段的用户访问情况。

配置逻辑：首先需要现场能解析这个域名，也就是说要放通DNS解析报文，然后放通这个域名，拒绝所有。

1 思路一

DNS服务器	114.114.114.114
test域名	www.test.com
test用户	172.16.10.0/24

2 思路二

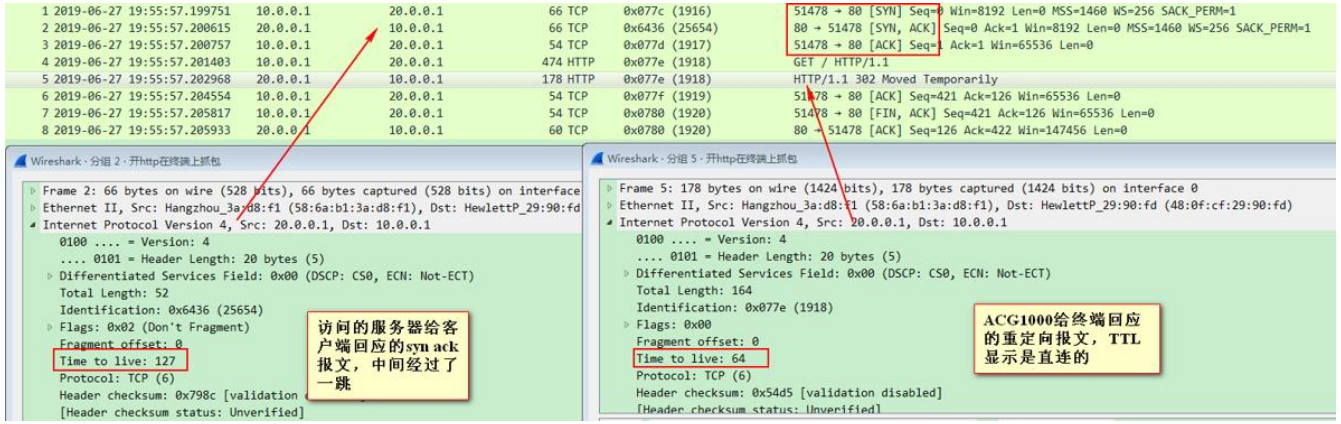
常见问题与维护（1）

- 经过ACG1000的业务丢包或者业务不通
  - 抓包查看报文是否到达ACG1000
  - Debug查看报文被丢弃的原因

```
H3C-ACG> enable
H3C-ACG# debug  dp drop
H3C-ACG#clear log debug    //清除已有的debug信息，再进行测试
H3C-ACG# display log debug
<2020-04-23 16:05:48> Packet dropped udp 192.168.1.132:1342 -> 10.0.1.44:3389: local
webauth is not http tuple // 报文被丢弃，因为该报文不是http报文，无法进行认证。
<2020-04-23 16:08:15> Packet dropped UDP 192.168.1.132:62482 -> 192.168.0.254:53: policy
default action deny    //报文被丢弃，因为默认策略为deny。
```

常见问题与维护（2）

- 本地web认证失败
  - 要求终端访问报文来回都过ACG1000。
  - 认证流量能否被识别成用户。
  - 桥模式部署时bvi口必须要配置地址。
  - 是否开启HTTPS弹portal。
  - 是否有弹portal页面的web服务器环境。



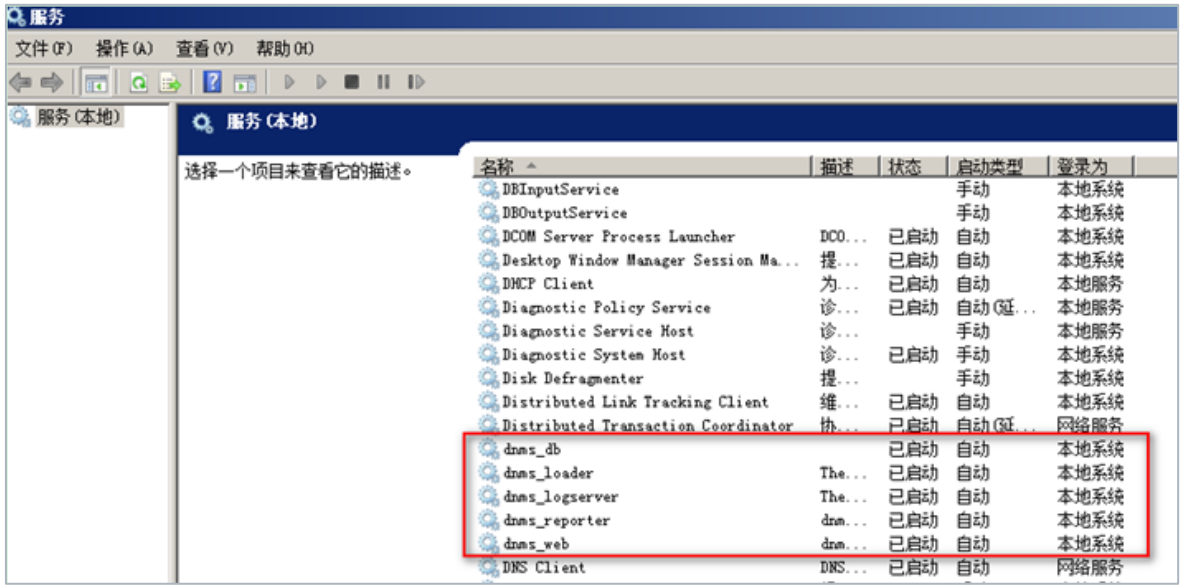

```
H3C-ACG> enable
H3C-ACG# configure terminal
H3C-ACG(config)# user-policy https-portal enable
```

常见问题与维护（3）

- ACG1000设备上没有产生应用审计等日志（保证配置正确并记录应用审计日志的前提下）
  - 设备上是否有特征库升级授权并将特征库升级到最新版本。
  - 设备上有没有存储介质用于存储日志。（支持U盘存储）
  - HTTPS类型的流量有没有开启解密策略。
  - 保证双向流量上设备并能被识别成用户。
  - 设备上该日志是否选择被记录。

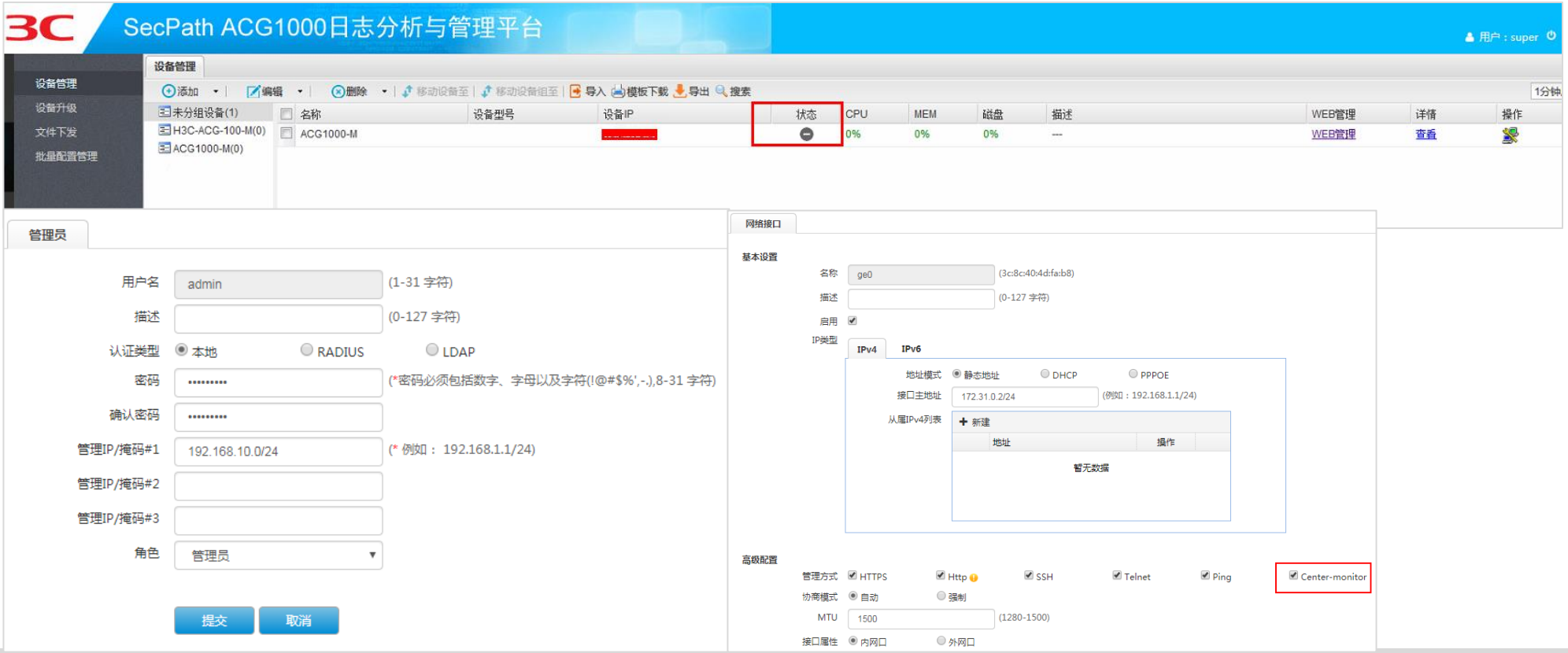
常见问题与维护（4）

- ACG日志分析管理平台上没有收到ACG1000发送过来的日志
  - 日志分析管理平台上是否有授权去纳管ACG1000设备。（出厂自带90天）
  - ACG1000设备是否产生日志，并且记录了该类型的日志。
  - ACG1000上日志主机配置是否正确，是否路由可达。
  - 通过在ACG1000上抓包确认日志是否已经发送到ACG日志分析管理平台。
  - 安装日志分析管理平台的服务器上安装了防火墙使得报文被丢弃。
  - 日志管理软件的五个进程（dnms_db、dnms_loader、dnms_logserver、dnms_reporter、dnms_web）是否都已经启动，必要时可以选择手动重启一下这些服务。（R0303版本）



常见问题与维护（5）

- ACG manager上显示ACG1000设备离线状态
  - 网管平台到ACG1000是否路由可达
  - ACG1000上是否配置了管理地址
  - ACG1000的管理口下面是否勾选Center-monitor
  - 网络中是否放通了TCP 8888端口报文



ACG1000常用定位命令

- H3C-ACG# display ip connection　　查看会话
- H3C-ACG# debug dp drop/error　　查看丢包原因
- H3C-ACG# debug aaa events　　查看认证情况
- H3C-ACG# debug application identify　　查看应用识别情况
- H3C-ACG# debug app audit log　　查看应用审计日志
- H3CACG1000# debug dp filter src-ip X.X.X.X dst-ip Y.Y.Y.Y

  H3CACG1000# debug dp basic　　查看报文的基本转发情况

www.h3c.com