

UNIS ACG1000 系列应用控制网关

用户 FAQ

目 录

1 部署方式 FAQ	1
1.1 ACG 应部署在哪里？	1
1.2 ACG 部署方式有哪些？	1
1.3 什么是路由模式？	1
1.4 路由模式使用在什么情况下？	1
1.5 路由模式下无法访问外网？	1
1.6 什么是透明模式？	1
1.7 透明模式无效果？	1
1.8 透明模式的工作原理？	2
1.9 透明模式的实用性在哪里？	2
1.10 什么是旁路模式？	2
1.11 使用旁路模式的好处是什么？	2
1.12 查看 ACG 日志信息为空时怎么处理？	2
1.13 部署 ACG 有什么好处？	2
1.14 为什么 ACG 配置正确但是数据无法通过？	2
2 设备管理 FAQ	2
2.1 为什么管理员用户不能通过 HTTP、SSH、或者 Telnet 登录设备，不显示 web 页面？	2
2.2 为什么 HTTPS 无法打开防火墙的 WEB 页面？	3
2.3 在“系统管理>管理员”，“添加管理员”页面中的“管理 IP/掩码”的作用是什么？	3
2.4 用户登录成功后，可在哪里修改密码？	3
2.5 默认 admin 管理员账户的密码如何重置？	3
2.6 什么是管理员双因子认证？	3
2.7 USBkey 支持哪些厂商？	3
2.8 更新 CA 根证书后 https 访问设备不能打开设备登录界面？	3
2.9 使用 IE 浏览器 https 无法访问设备 WEB 界面？	3
2.10 火狐浏览器默认不能调用 Ukey 中的证书？	4
3 应用审计 FAQ	4
3.1 如何查看当前的应用审计策略？	4
3.2 应用审计可以做关键字过滤吗？	4
3.3 应用审计日志可以存储多少条？	4
3.4 应用审计日志按照时间查询多天日志时，为什么会有空白页？	4
3.5 为什么应用审计不报日志？	4

3.6 为什么访问网站未记录网站访问日志？	4
3.7 为什么恶意 URL 白名单不生效？	5
3.8 为什么远程 syslog 服务器收不到日志？	5
3.9 邮件日志中为何有的邮件日志对应的是下载按钮，有的邮件日志对应是查看按钮？	5
3.10 为何邮件日志中有时看不到查看的按钮？	5
4 用户信息中心 FAQ.....	5
4.1 当用户中心用户识别错误的时候，同时用户数已经达到了用户中心的规格数，如何操作？	5
4.2 为何用户中心的应用日志数有时会多于日志链接的日志页面的总数？	5
4.3 当用户很大时，特定用户的信息为何没有更新？	5
4.4 当用户流量很大时，特定用户的审计日志统计信息统计为 0？	6
4.5 当用户数量很大时，停流 40 分钟后 CPU0 仍然很忙，显示为 100%？	6
4.6 为何用户流量统计有时会出现某应用类的应用未显示在饼图中？	6
4.7 为何网站访问分析总数有时会比该用户网站日志总数少？	6
4.8 为何用户在线时长有时会比在线用户显示的时长少？	6
4.9 为何用户中心在线时长有时会比在线用户显示的时长多？	6
4.10 用户中心用户的排名是按照什么方式？	6
4.11 为何用户的应用行为不能记录到时间？	6
4.12 为何在无线环境下在用户中心看到的账号信息不正确？	7
4.13 为什么用户信息中心只记录部分审计日志计数后不入库了？	7
5 流控 FAQ	7
5.1 带宽的上下行如何区分？	7
5.2 配置最大带宽和保障带宽为何无法成功？	7
5.3 流量控制通道有多个匹配条件时如何匹配？	7
5.4 最大带宽和保障带宽分别有什么作用？	7
5.5 配置了保障带宽但是在拥塞时流量无法达到其保障带宽？	8
5.6 配置了多个流量控制通道，只有第一个通道有流量匹配？	8
5.7 什么是流量排除策略？	8
5.8 每 IP 限速和通道带宽限制的处理关系？	8
5.9 如何限制 P2P 的流量？	8
5.10 流量控制通道的高、中、低级别有何作用？	8
5.11 子通道的保障带宽总和大于父通道保障带宽，如何分配保障带宽？	8
5.12 线路整体带宽仍然有富裕，部分应用延时很大？	8
5.13 QOS 通道带宽自适应？	8
5.14 QOS 通道带宽百分比范围？	9
5.15 QOS 通道带宽联动？	9
5.16 QOS 通道自适应算法说明	9

5.17 QOS 通道自适应每 IP 和每用户说明	9
5.18 QOS 透明部署配置 Qos 时，线路绑定说明	9
5.19 QOS 三层部署配置 Qos 时，线路绑定说明	9
5.20 QOS 子接口部署配置 Qos 时，线路绑定说明	10
5.21 QOS 聚合接口部署配置 Qos 时，线路绑定说明	10
5.22 如何定位 QoS 策略是否被命中，命中哪条 QoS 策略？	10
5.23 如何定位数据包是否被 QoS 策略丢弃？	10
6 设备流量统计 FAQ	10
6.1 设备流量统计的值为何比实际数据包的速率小？	10
6.2 设备流量统计为何与用户流量统计有所出入？	10
6.3 设备异常掉电后，为何丢失了部分数据？	10
6.4 更改系统时间对设备流量统计会产生哪些影响？	10
6.5 接口状态页面，没有完全显示所有接口的状态信息？	11
6.6 接口状态页面上有接收或发送速率的信息，但健康统计页面整机转发流量无数据？	11
6.7 设备健康统计页面，整机转发流量只能看到上行或者下行的流量信息？	11
6.8 接口状态页面的数据，多长时间更新一次？	11
7 策略路由 FAQ	11
7.1 什么是策略路由？	11
7.2 同一条策略路由最多支持几个下一跳？同时配置多个下一跳的情况下，如何转发报文？	11
7.3 策略路由转发流程图	12
7.4 策略路由由下一跳不可达的判断条件是什么？	12
8 ISP 路由 FAQ	13
8.1 什么是 ISP 路由？	13
8.2 ISP 路由的工作环境是什么？	13
8.3 ISP 路由是怎样工作的？	13
8.4 ISP 路由如何进行流量负载均衡？	13
8.5 ISP 路由和静态路由有什么区别？	13
9 IPsec VPN FAQ	14
9.1 如何查看当前 IKE SA 信息？	14
9.2 如何查看当前 IPsec sa 信息？	14
9.3 IPsec VPN 中报文的默认加密方式是什么？	14
9.4 一条 VPN 最多支持多少条隧道？	14
9.5 为什么 IPsec VPN 第一阶段协商不成功？	15
9.6 为什么 IPsec VPN 第二阶段协商不成功？	15
9.7 为什么保护子网不能通讯？	15
9.8 为什么某些移动终端接入 VPN 不成功？	15

9.9 NAT 环境下 IPSEC 协商不成功？	15
9.10 IPSEC 建起连接后，一端断开后，IPSEC 无法协商？	16
9.11 本端 SA 状态显示连接，流量无法转发？	16
9.12 当设备存在多出口时，其它参数正确，IPSEC 协商失败？	16
9.13 IPSEC 使用国密证书协商不成功？	16
9.14 IPSEC 快速配置与 IPSEC VPN 标准配置有什么区别？	16
9.15 IPSEC 快速配置一阶段和二阶段默认参数？	16
9.16 IPSEC 快速配置默认参数支持修改吗？	17
9.17 IPSEC 预共享密钥有字符限制么？	17
9.18 主链路断开后为什么 ipsec 链路没断开？	17
9.19 主链路被引用后还能继续当做其他链路的备链路吗？	17
9.20 主备切换必须等待 ipsec 老化时间结束才能切换吗？	17
9.21 主链路选择连接方式为监控链路故障自动连接后主链路选择下拉为什么为空？	18
9.22 链路断开是监控哪个阶段？	18
9.23 使用测试仪打单向流量，一条隧道的情况下为什么解密端 cpu0 核使用率很高？	18
9.24 IPSEC 场景，DPD 未开启的情况下，ipsec 关联的物理接口 down 后，ike 和 ipsec sa 不会跟随断开连接？	18
10 IPv6 FAQ	18
10.1 配置 IPv6 有什么优点？	18
10.2 什么是 IPv6 邻居发现协议？	18
10.3 IPv6 中的路由器请求报文作用（Router Solicitation）？	19
10.4 IPv6 中的路由器通告报文作用（Router Advertisement）？	19
10.5 邻居请求（Neighbor Solicitation）报文作用？	19
10.6 邻居通告（Neighbor Advertisement）报文作用？	19
10.7 邻居发现协议的功能是什么？	20
10.8 在配置 IPv6 静态路由之前，需完成以下任务？	20
10.9 IPv6 缺省路由的生成方式？	20
10.10 在 Tunnel 接口上配置了相关的参数后（例如隧道的起点、终点地址和隧道模式）仍未处于 up 状态？	20
10.11 6to4 隧道是否需要配置目的地址？	20
10.12 ISATAP 隧道是否需要配置目的地址？	20
10.13 从设备端执行什么配置去主动 ping 另一台设备的 IPv6 地址？	21
10.14 什么是 IPv6 手动隧道？	21
10.15 什么是 6to4 自动隧道？	21
10.16 什么中 ISATAP 自动隧道？	21

11 VRF FAQ	21
11.1 不同的 VRF 间如何相连?	21
11.2 ACG1000 最多可以创建多少个 VRF?	22
11.3 VRF 基本设计概念是什么?	22
11.4 路由表隔离功能的逻辑?	22
11.5 流表的隔离功能?	22
11.6 VRF 模块设计背景?	22
12 动态路由 FAQ	22
12.1 RIP 支持 v1 和 v2 功能吗?	22
12.2 RIP 开启时默认是 V1 还是 V2 版本?	22
12.3 OSPF 是否支持 pppoe 接口?	22
12.4 OSPF 的 Router ID 如何配置, 缺省是什么?	23
12.5 OSPF 没有路由, 甚至邻居都不能形成 Full 关系, 最常见的原因是什么?	23
12.6 有什么好的办法知道 OSPF 出了问题?	23
12.7 OSPF 如何自动计算接口 cost 的?	23
12.8 OSPF 链路两端配置不同的网络类型, 能否形成 Full 关系?	24
12.9 OSPF 路由聚合是否可以跨区域聚合?	24
12.10 OSPF 的 Virtual-Link 是否很有用处?	24
12.11 OSPFv3 在界面中是否有配置选项?	24
12.12 OSPFv3 邻居无法建立?	24
12.13 OSPFv3 路由信息不正确?	25
12.14 当执行 no router ospf6 后, 其它接口有关 ospfv3 配置是否自动删除?	25
13 HA FAQ	25
13.1 配置 HA 的优点?	25
13.2 HA 的工作模式	25
13.3 什么是 HA 的主备模式?	25
13.4 什么是 HA 的主主模式?	25
13.5 HA 工作状态	26
13.6 HA 接口概念	26
13.7 抢占模式	26
13.8 抢占延时定时器	26
13.9 心跳报文	26
13.10 HA 管理地址	27
13.11 HA 状态同步	27
13.12 HA 主备状态切换	27
13.13 HA 主主状态切换	27

13.14 HA 主主邻居为什么建立不起来	27
13.15 HA 主主地址代理	27
13.16 HA 主主非对称路由	28
13.17 HA 主备场景下执行手动同步配置，备设备重启完成后，主设备 HA 监控仍显示配置不同？	28
14 Bypass FAQ	28
14.1 每台设备最多有多少组 Bypass 接口？	28
14.2 Bypass 接口使用在何种网络场景中？	28
14.3 Bypass 功能默认开启吗？	28
14.4 进程异常时是否会触发 Bypass？	28
14.5 系统运行过程断电是否会触发 Bypass？	28
14.6 系统启动过程中是否会持续 Bypass 状态？	28
14.7 从系统正常到掉电进入 Bypass 状态时，会丢几个 ICMP 报文？	28
15 APP 缓存 FAQ	29
15.1 APP 缓存能缓存哪些文化类型？	29
15.2 APP 模糊匹配 URL 如何设置？	29
15.3 本地文件如果不存在怎么办？	29
15.4 App 缓存文件存储在哪里？	29
15.5 为什么重启后 app 缓存计数不正确？	29
15.6 APP 动态缓存的规格？	29
15.7 URL 链接为什么无法提交？	29
15.8 CLI 下上传的文件能大于剩余缓存空间？	29
15.9 磁盘空间大于 80%，设备是否还能正常上传 app 文件？	29
15.10 页面上动态缓存域名下的已经下载的多个 app 缓存文件，能否单独删除其中一个 app 缓存文件？	30
15.11 动态缓存的 app 文件类型？	30
15.12 文件名包含中文时 APP 动态缓存失败？	30
15.13 应用缓存功能在 PC 端连续下载两次文件，缓存计数只命中一次，一次在设备下载，一次在 server 下载？	30
15.14 Smartbits 打入混合流量，设备的内存占用较高，此时导入应用缓存，WEB 或者 Console 概率出现错误提示，WEB 会处于一直上传的状态？	30
16 会话限制 FAQ	30
16.1 会话限制基于什么原则来进行限制？	30
16.2 配置两条会话限制，引用的地址对象分别都包含了某个 IP 地址，但是会话限制的配置不同，那么该以哪一个为标准？	31
16.3 会话限制是否可以只限制会话总数，而不限制新建会话速度？	31
16.4 同一个地址对象是否可以配置多个会话限制？	31

16.5 在配置会话限制之前，地址对象的会话总数已经超过了该会话限制的会话总数，那么配置该条会话限制后是否会将会话数保持在限制的数目下？	31
17 DNS 代理 FAQ	32
17.1 display dns statistics 介绍	32
17.2 dns 规格	32
17.3 dns session 功能	32
17.4 dns 缓存达到 5w 规格后，对新来的 dns 请求处理	32
17.5 DNS 报文数据段>512 后，dns 处理	32
17.6 DNS 接口类型改变后 dns 无法解析	32
17.7 DNS A 记录显示	32
17.8 DNS cache 显示	32
17.9 开启 DNS 透明代理的功能，无法上网	33
17.10 域名比较长，页面查询这样的域名是无法查询	33
17.11 设备直接 ping 域名	33
17.12 设备 dns 流程	33
17.13 dns-proxy debug 说明	33
17.14 DNS 多链路基于负载	33
17.15 多链路 DNS 基于优先级	34
17.16 为什么进行包含域名的策略控制会放行一段时间后才可匹配策略？	34
17.17 客户端 A 没有配置设备为 DNS 代理，客户端 B 配置设备为 DNS 代理，客户端 A 发出经过设备的 DNS 请求，之后客户端 B 也发出相同域名的 DNS 请求，设备在对 B 的请求处理过程是怎样的？	34
18 攻击防护 FAQ	34
18.1 扫描攻击防御中的黑名单作用是什么？	34
18.2 配置满规格黑名单后，重复提交 IP 地址为什么还能提交成功？	34
19 统计集 FAQ	35
19.1 统计集统计最近 1 小时、最近 1 天、最近 1 周数据统计的刷新闻隔是多少？	35
19.2 统计集应用流量统计中所显示的流速计算？	35
19.3 统计集用户统计中用户的类型？	35
19.4 统计集统计用户及应用的规格？	35
19.5 统计集中总流量是如何计算的？	35
19.6 统计集中刷新按钮的作用？	35
19.7 上行流量和下行流量如何区分？	35
19.8 统计集数据是否支持 HA？	35
19.9 统计集数据保存重启后是否会丢失？导出再导入是否会丢失？	36
19.10 饼图默认显示 Top 多少？其它应用是什么？	36
19.11 统计集中是否会统计出到本地流量？	36

19.12 当统计集显示页面放大或缩小时，饼图显示变化？	36
19.13 统计集是否支持旁路模式？	36
19.14 统计集中应用统计与用户统计查看区别？	36
20 地址探测 FAQ	36
20.1 如何配置 track？	36
20.2 为什么 ping 类型的 track 状态不稳定？	36
20.3 为什么 tcp 类型的探测不成功？	36
20.4 为什么 dns 类型探测失败？	37
20.5 ACG 配置 HA 并且关联 track，主墙无法切换？	37
20.6 HA 联动备墙无法跨网段探测？	37
20.7 WEB 页面导入 csv 格式用户和用户组无法同步？	37
21 策略优化 FAQ	37
21.1 七元组策略按照什么顺序进行匹配？	37
21.2 单条七元组审计策略中的应用审计规则、URL 审计规则按照什么顺序进行匹配？	37
21.3 添加或修改七元组策略会有什么影响？	38
22 IMC 联动 FAQ	38
22.1 如何排查用户无法登录 IMC 服务器管理页面？	38
22.2 为什么认证时无法接收认证推送页面？	38
22.3 使用 NAT 用户通过认证后访问外网页面依然弹出认证页面，导致循环认证？	38
22.4 为什么认证时，可以接收推送认证页面，用户名密码输入完毕后无法认证成功？	38
22.5 为什么用户认证时点击一次上线，显示设备拒绝请求，点击多次后可认证成功？	38
22.6 登录超时后重新认证，在认证窗口填写用户名密码后点击“上线”提示“用户已在线”？	39
22.7 为什么认证模板设置 IE10 浏览器没有调色板按钮，只能通过数字设置认证按钮颜色？	39
22.8 用户在线时间超出所配置的超时时间，有时可下线、有时不可下线？	39
23 第三方用户存储认证	39
23.1 如何排查用户无法登录 Radius（IMC）服务器管理页面？	39
23.2 为什么认证时无法重定向到认证页面？	39
23.3 输入用户名及密码后，认证失败，提示“用户名或密码错误”，如何定位认证失败原因，并及时修改？	40
23.4 在页面认证服务器>本地 Web 认证页面，在用户登录唯一性检查项，配置单一账号登录，并禁止禁止同名用户再次登录后，为什么用户第三方 Radius 认证对于同一账号仍能多次登录？	40
24 断点续传 FAQ	40
24.1 什么情况下属于断点续传？	40
25 会话统计 FAQ	40
25.1 会话统计排名为什么只有前 50 个？	40
25.2 会话监控页面有的会话存在时间为 0 秒？	40

26 抓包工具 FAQ	41
26.1 抓包工具开始抓包后，什么情况下停止抓包？	41
26.2 抓包工具高级选项里的抓取新建会话是什么意思？	41
27 日志分析与管理平台部署方式 FAQ	41
27.1 ACG1000 日志分析与管理平台运行环境要求有哪些？	41
27.2 ACG1000 日志分析与管理平台有哪些端口被占用？	41
27.3 ACG1000 日志分析与管理平台管理员客户端有哪些要求？	41
27.4 安装完成后打不开 ACG1000 日志分析与管理平台提示端口被占用怎么办？	41
27.5 如何设置映射端口使 ACG1000 日志分析与管理平台可以接收到 ACG 设备的信息？	42
27.6 ACG1000 添加到管理平台后，点击 ACG1000 页面的“数据中心”无法打开？	42
28 日志分析与管理平台程序管理 FAQ	42
28.1 ACG1000 日志分析与管理平台默认登录用户名和密码是什么？	42
28.2 ACG1000 日志分析与管理平台的 SYSLOG 端口是多少？	42
28.3 ACG1000 日志分析与管理平台使用什么浏览器比较好？	42
28.4 打开 ACG1000 日志分析与管理平台登录界面看不到验证码怎么办？	43
28.5 打开 ACG1000 日志分析与管理平台接收不到日志怎么处理？	43
28.6 用户登录后可以在哪里修改密码？	43
28.7 用户打不开 ACG1000 日志分析与管理平台怎么办？	43
29 日志分析与管理平台设备管理 FAQ	43
29.1 如何添加设备？	43
29.2 如何查看添加到设备组的设备？	43
29.3 正确添加好设备后为什么设备状态显示未在线设备？	43
29.4 最多可以管理多少台设备？	44
29.5 如何在 ACG1000 日志分析与管理平台直接进入设备管理界面？	44
29.6 如何能够更方便的管理设备？	44
29.7 导出设备管理是全部导出，还是只导出某一组的设备？	44
29.8 如果设备突然掉线了怎么办？	44
29.9 想将设备进行重启，怎么操作？	44
29.10 当设备太多了，找不到想管理的设备怎么办？	44
29.11 设备添加信息错误了，如何修改？名称可以修改吗？	44
29.12 如果删除此设备后，之前此设备的日志还存在吗？	44
29.13 如何通过 EXCEL 导入设备	45
29.14 如何使用自动探测和自动下发文件功能？	45
29.15 是否支持所有的 URL 格式的自动探测？	45
29.16 日志分析与管理平台对服务器内存是否有要求？	45

30 日志分析与管理平台监控统计 FAQ	45
30.1 监控统计都包括哪些信息？	45
30.2 在监控统计中可以调节的参数有哪些？	45
30.3 系统状态包括哪些信息？	45
30.4 设备流量监控包括哪些信息？	46
30.5 用户排名流量监控包括哪些信息？	46
30.6 应用流量监控包括哪些信息？	46
30.7 不同范围的波形图的时间间隔是多少？	46
30.8 某一台客户端查询不到设备流量，但是另外一台管理相同设备的 ACG1000 日志分析与管理平台却可以查询的到，这是什么原因？	46
31 日志分析与管理平台策略管理 FAQ	47
31.1 地址对象的基本操作都有哪些？	47
31.2 服务对象的基本操作都有哪些？	47
31.3 时间对象的基本操作都有哪些？	47
31.4 应用对象的基本操作都有哪些？	47
31.5 URL 对象的基本操作都有哪些？	47
31.6 关键字对象的基本操作都有哪些？	48
31.7 集中策略如何下发？	48
31.8 如何查看下发失败原因？	48
31.9 策略成功下发在设备端哪里可以找到？	48
31.10 可以同时多个策略下发吗？	48
31.11 可以对策略进行什么操作？	48
32 日志分析与管理平台日志查询 FAQ	48
32.1 日志查询有哪些作用？	48
32.2 日志查询是通过什么来查询数据的？	48
32.3 如何进行日志查询？	49
32.4 正确的查询步骤，为什么没有日志？	49
32.5 日志查询都可以设置哪些过滤条件？何时使用？	49
32.6 日志查询的效率受哪些因素的影响？	49
33 日志分析与管理平台统计报表 FAQ	50
33.1 统计报表有哪些作用？	50
33.2 报表文件，报表任务，预定义报表任务都是用来做什么的？	50
33.3 设备状况为未选设备，无法生成报表是什么情况？	50
33.4 产生的报表文件都有什么格式的？	50
33.5 报表任务可以选择几台设备？	50
33.6 点击立即执行，为什么没有报表文件？	50

34 日志分析与管理平台系统管理 FAQ	51
34.1 在哪里修改管理员密码？	51
34.2 能否自己为管理员分配权限？	51
34.3 如果其他新建管理员忘记密码如何找回？	51
34.4 如何备份数据库？	51
34.5 如何还原数据库？	51
34.6 如何进行日志备份？	51
34.7 如何进行日志还原？	51
34.8 数据库配置自动备份后存放在哪里？	51
34.9 数据库备份结果页面显示哪些信息？	51
34.10 数据库备份还原注意事项有哪些？	52
34.11 设备批量重启增加哪些功能？	52
35 服务质量管理 FAQ	52
35.1 服务质量管理条目“最后一次成功率”和“最后一次延时”在建立前的时间也有数据显示？	52
35.2 为什么 tcp 类型的服务质量管理条目探测结果为零？	52
35.3 为什么 dns 类型的服务质量管理条目探测数据一直为零？	52
35.4 为什么 debug service-quality 不显示 dns 类型的服务质量管理条目发送的探测报文？	52
36 基于用户 MAC 的转发策略 FAQ	52
36.1 在 ACG 上配置有用户认证策略，并新建用户将 PC 的 MAC 地址绑定，为什么 PC 仍无法上网并重定向到认证页面？	52
37 链路负载均衡 FAQ	53
37.1 负载均衡使用场景？	53
37.2 负载均衡支持的负载方式？	53
37.3 带宽比的负载方式使用的算法？	53
37.4 带宽比负载使用条件？	53
37.5 优先级定义	54
37.6 负载方式为优先级的使用条件？	54
37.7 会话保持与带宽比结合使用	54
37.8 会话保持与优先级	54
37.9 过载保护使用说明？	54
37.10 健康检查	54
38 三权分立 FAQ	54
38.1 三权模式下各管理员的职责？	54
38.1.1 三权模式可以切换到普通模式吗？	55
38.2 三个默认管理员账号是否可编辑？	55
38.3 普通模式切换到三权模式后，原来的系统管理员、审计员账号还可以登录吗？	55

39 广告推送 FAQ	55
39.1 广告对象规格	55
39.2 广告策略规格	55
39.3 广告策略引用广告对象规格	55
39.4 广告对象里图片规格及限制	55
39.5 广告策略引用广告对象限制	55
39.6 广告对象命令行限制	55
39.7 广告策略引用对象位置	56
39.8 广告对象和广告策略里设备 IP 的使用	56
39.9 域名白名单匹配规则	56
39.10 手机端广告图片展示限制	56
39.11 广告策略跨网段使用限制	56
39.12 手机端浏览器使用限制	56
39.13 微博类网站广告使用限制	56
39.14 一些网站不弹广告	56
39.15 邮箱类不弹广告	56
39.16 开启广告推送后，一些网页打不开	57
39.17 HA 主备环境下广告推送使用	57
39.18 广告图片展示时间	57
39.19 广告设置白名单规格	57
39.20 广告策略匹配顺序	57
39.21 广告策略里启用按钮和推送按钮的作用	57
39.22 广告对象图片上传大小	57
39.23 手机端广告对象限制	57
39.24 Edge 浏览器不支持广告推送	57
39.25 推送广告网站类型	57
39.26 广告对象里图片不能全部删除	58
39.27 今日头条 app 不推送广告	58
39.28 https 网站类型使用 http 方式访问网页打不开	58
39.29 开启广告推送后访问部分网站但是过了几秒网页变成黑色	58
39.30 广告推送只对域名方式的 URL 生效？	58
40 跨三层 mac 学习 FAQ	58
40.1 设备学习不到交换机 mac 地址？	58
40.2 新增的 IP/MAC 条目设备不能及时学习到该 IP 的数据如何处理？	58
40.3 如果交换机的 MAC 不在扫描列表中用户数据处理流程？	58
40.4 如果交换机的 MAC 在扫描列表中用户数据处理流程？	59

40.5 多个交换机时如何学习扫描?	59
40.6 每次扫描的结果如何处理?	59
40.7 跨三层 MAC 扫描的学习过程是什么?	59
40.8 快速老化机制是什么?	59
40.9 老化定时器的工作原理?	59
40.10 SNMP 跨三层学 MAC 交换机规格是多大?	59
41 防共享 FAQ	60
41.1 防共享终端显示与实际终端型号不一致?	60
41.2 一个热点下多台小米手机未识别出是共享终端?	60
41.3 HA 环境防共享监控用户列表不能同步到备设备?	60
41.4 阻断提示中<frozen-time>单位如何处理?	60
42 认证策略 FAQ	60
42.1 认证策略支持配置哪几种认证方式?	60
42.2 混合认证支持哪几种认证方式?	60
43 微信认证 FAQ	60
43.1 为什么认证时无法重定向到认证页面?	60
43.2 苹果手机无法自动弹出 portal?	61
43.3 移动端弹出 portal，并点击一键微信连 wifi 后，认证失败，如何定位认证失败原因，并及时修改?	61
43.4 若环境中无线路由器为 cisco 无线路由器，且支持 2.4G 和 5G 信号，假设 ssid 分别为 cisco 与 cisco-5G，此时应该连接哪个 ssid?	61
43.5 部分安卓手机弹出 portal 页面，点击一键微信连 WIFI 后，页面无反应或者会有提示信息“该浏览器不支持自动跳转微信请手动打开微信”，应如何解决?	61
43.6 微信认证页面配置是否支持 HA 检查?	61
43.7 微信认证用户是否支持 HA 主备、HA 主主同步?	61
43.8 若一台 ACG 下挂两台 AP，AP1 有在微信公众平台上注册，而 AP2 没有注册；此时 ACG 上微信认证策略为全 any 时，若用户连接 AP2 的 ssid 时，不能正常认证成功，只有连接 AP1 的 ssid 时才能正常认证成功；此时如何满足此类组网?	61
43.9 微信认证成功后，在用户信息中心中查看微信图像没有加载成功，如何定位?	62
43.10 微信认证不支持双频 AP 的两个信号同时接入?	62
43.11 微信认证单台设备下支持多个 SSID?	62
43.12 微信认证是否支持 HTTPs 弹 portal?	62
43.13 微信认证有些安卓手机扫码连接 wifi 后出现网络连接失败现象?	62
43.14 PC 推荐浏览器?	62
43.15 移动终端推荐浏览器?	62
43.16 设备上的 WiFi 名称不支持中文?	63
43.17 微信连 wifi 未认证情况下用户微信能收发消息?	63

43.18 微信内置浏览器访问部分公众号不能弹出 Portal 页面？	63
43.19 苹果手机不能通过 3G/4G 实现扫码认证？	64
43.20 微信连 wifi 强制关注功能支持订阅号吗？	64
43.21 微信连 wifi 何时需要设置 token-url？	64
43.22 微信连 wifi 电脑端弹出的 portal 微信二维码一段时间后超时，提示：服务器繁忙请一分钟后刷新重试？	64
44 用户源 MAC 日志显示 FAQ	64
44.1 用户源 MAC 如何获取？	64
45 免认证 FAQ	65
45.1 免认证用户不需要认证账号？	65
46 无感知认证 FAQ	65
46.1 什么是无感知认证？	65
46.2 无感知认证超时时间计算标准？	65
46.3 无感知认证支持跨三层组网吗？	65
46.4 哪几种方式支持无感知？	65
46.5 无感知在哪些情况下生效？	65
47 混合认证 FAQ	66
47.1 什么是混合认证？	66
47.2 混合认证能选择单一的认证方式吗？	66
47.3 混合认证的模板和其他认证一样吗？	66
48 短信认证 FAQ	66
48.1 用户使用浏览器 A 获取短信验证码，在浏览器 B 上输入手机号和验证码，是否能短信认证成功？	66
48.2 设备导出设备配置，是否包含短信认证配置？	66
48.3 双机主备环境，主设备配置短信认证，备设备是否同步短信认证的配置？	66
49 微信白名单 FAQ	66
49.1 微信白名单是什么？	66
49.2 微信白名单和全局白名单有什么不同？	67
49.3 微信白名单对混合认证中的微信认证方式生效吗？	67
50 https 弹 portal	67
50.1 什么是 https 弹 portal？	67
50.2 安卓手机 https 弹 porta 警告非安全怎么办？	67
50.3 https 弹出 portal 以后没有认证为什么可以正常打开网页？	67
50.4 https 弹 portal 支持所有 https 域名 url 吗？	67
50.5 为什么在浏览器上通过导航网站访问 https 类型网站时没有弹 portal？	68
50.6 怎样能使 https 类型的网站弹 portal？	68

50.7 浏览器多次访问 https 页面，会出现弹出认证页面很慢的情况？	68
50.8 访问 https 类型网站时有的浏览器无法弹出 portal 认证界面？	68
50.9 默认不使能 https 弹 portal 功能？	68
51 伪 Portal 抑制 FAQ	68
51.1 伪 portal 抑制原理是什么？	68
51.2 refresh 重定向是一定起作用吗？	68
51.3 refresh 重定向能有效抑制所有的软件吗？	69
52 强制关注 FAQ	69
52.1 什么是强制关注？	69
52.2 第一次上线是否需要先关注公众号？	69
53 认证模板设置 FAQ	69
53.1 什么是认证模板设置？	69
53.2 认证模板预览有认证方式切换功能？	69
54 策略查找 FAQ	69
54.1 策略查找支持哪几个维度？	69
55 地址本域名 FAQ	70
55.1 什么是地址本域名？	70
55.2 地址本域名在策略中引用后不生效？	70
56 NAT44 FAQ	70
56.1 NAT44 支持端口利用吗？	70
56.2 NAT44 端口分配规则？	70
57 4G 上网卡 FAQ	70
57.1 目前支持哪些型号 4G 上网卡？	70
58 PPPOE 拨号 FAQ	71
58.1 设备 CPU100%情况下停流后仍然不能成功拨号？	71
59 新版本链路负载均衡 FAQ	71
59.1 负载均衡配置规格？	71
59.2 负载均衡支持的负载方式？	71
59.3 权重的负载方式使用的算法？	71
59.4 权重的负载使用条件？	71
59.5 优先级定义	71
59.6 负载方式为优先级的使用条件？	72
59.7 会话保持使用说明？	72
59.8 过载保护使用说明？	72
59.9 健康检查	72

59.10 链路负载均衡出接口配置说明？	72
59.11 免负载均衡地址使用说明？	72
59.12 负载均衡策略匹配条件-匹配应用使用说明？	72
59.13 负载均衡，策略路由，静态路由匹配顺序？	72
59.14 负载均衡流量匹配说明？	73
59.15 负载均衡的 ISP 地址配置说明？	73
60 用户/用户组优化 FAQ	73
60.1 用户/用户组的规格？	73
60.2 用户页面能否完整显示 8 个所属用户组？	73
60.3 用户组引用用户的个数规格？	73
60.4 用户/用户组的移动？	73
60.5 用户/用户组的导入导出？	73
61 LDAP 服务器同步 FAQ	74
61.1 异常 AD 域用户名同步到设备的处理	74
61.2 LDAP 服务器同步端口？	74
61.3 LDAP 组的作用？	74
61.4 LDAP 绑定方式对同步用户的影响？	74
61.5 LDAP 同步用户的限制？	74
61.6 LDAP BaseDN 写法？	74
61.7 被策略引用的远端用户被删除时，策略的变化	74
61.8 使用 LDAP 用户认证通过后，在服务器删除认证用户并在设备上同步该 OU？	74
61.9 HA 主备环境下 LDAP 同步支持？	74
61.10 IPSec 使用 LDAP 认证？	75
61.11 LDAP 自动时间？	75
62 端口镜像 FAQ	75
62.1 端口镜像规则有哪些配置限制	75
62.2 配置端口镜像后并未镜像出业务流量	75
62.3 配置端口镜像后只镜像出了部分业务流量	75
62.4 如何配置将多个接口的流量镜像到同一个监控接口	75
62.5 是否支持远端镜像功能	76
62.6 使用设备上的抓包工具是否能够抓取到监控接口镜像过来的业务报文	76
62.7 如何查看镜像功能是否生效	76
62.8 是否可以配置将万兆口流量镜像到千兆口或千兆口流量镜像到百兆口	76
63 解密策略 FAQ	76
63.1 设备开启 https 解密后，电脑必须要安装设备上导出的证书吗？	76
63.2 电脑端证书如何导入？	76

63.3 证书的有效期是否影响解密？	76
63.4 设备 DNS 设置全局模式时，为什么显示的证书不是颁发证书？	76
63.5 为什么安装证书以后，chrome 浏览器访问 12306 网站显示非安全连接？	77
63.6 两台防火墙串联，用户电脑应该导入哪一台的证书？	77
63.7 防火墙的证书一定要和用户导入证书一致吗？	77
63.8 防火墙下连的无线设备，手机端也需要导入证书吗？怎么导入？	77
63.9 所有邮箱客户端都支持审计吗？	77
63.10 配置 Https 解密后百度页面打不开？	77
63.11 https 解密审计对移动终端生效吗？	77
63.12 https 解密策略开启后，移动终端 APP 无法访问网络？	77
64 DDNS 功能 FAQ	78
64.1 DDNS 规格限制	78
64.2 当公网口存在多个 IP 时使用哪个 IP 地址？	78
64.3 DDNS 配置了更新某一特定域名，为什么此账户下的所有域名地址都进行了更新？	78
64.4 DDNS 与 DNS 功能模块功能关系？	78
65 DNS-DNAT 功能 FAQ	78
65.1 DNS-DNAT 规格	78
65.2 如果设备同时开启 dns 透明代理和 dns-dant 功能，DNS 报文如何处理？	78
65.3 DNS-DNAT 探测功能是什么？	79
65.4 如何查看 DNS 服务器是否正常状态？	79
66 多配置管理功能 FAQ	79
66.1 配置文件限制	79
66.2 配置文件保存在哪？清除配置重启时是否会清除掉配置文件？	79
66.3 如何查看我保存的配置文件？	79
66.4 在使用 ftp 方式导出配置文件时为什么配置了服务器地址和文件名称后面还提示输入服务器地址？	79
67 Portal 逃生 FAQ	80
67.1 设备 portal 逃生用户根据设备内存大小来设置存储规格？	80
67.2 portal 逃生功能开启，全局逃生模式的含义？	80
67.3 portal 逃生功能开启，已认证用户逃生模式的含义？	80
67.4 portal 逃生存储用户数达到规格时设备如何更新？	80
67.5 portal 逃生功能什么时候生效？	80
68 零配置上线 FAQ	81
68.1 零配置启动盘格式？	81
68.2 零配置启动盘文件结构？	81
68.3 零配置启动盘生效后能作为硬盘吗？	81

68.4 零配置启动盘里根目录下的 version 和序列号文件夹里 version 有什么差别？	81
68.5 设备运行阶段插入零配置上线 U 盘有影响吗？	81
68.6 零配置启动盘只能生效一次吗？	82
68.7 零配置启动盘失败会有提示吗？	82
68.8 零配置启动盘只能针对一台设备吗？	82
68.9 零配置启动盘序列号文件夹下启动配置和备份配置分别支持几个？	82
69 审计日志导出 FAQ	82
69.1 同一设备可以同时导出多个类型日志吗？	82
69.2 审计日志包括哪些类型？	82
69.3 审计日志可导出所有时间的日志吗？	82
69.4 审计日志导出支持负载内容导出吗？	82
69.5 所有设备都能导出审计日志吗？	82
69.6 审计日志有规格限制吗？	83
69.7 如果近一周审计日志的某天是没有日志，还能导出来吗？	83
69.8 修改系统时间小于当前时间后，导出今天的审计日志实际导出的是其他日期的日志？	83
70 业务告警 FAQ	83
70.1 配置完邮箱服务器怎么关闭该功能？	83
70.2 会话警告阈值规格是按照什么统计的？	83
70.3 邮箱服务器发送地址用户密码是指邮箱登录密码吗？	83
70.4 配置了邮箱服务器但是没有收到邮件？	83
70.5 邮箱服务器重置配置没有清空？	83
70.6 告警日志弹窗会在任何界面弹出吗？	84
70.7 告警日志记录最大规格？	84
71 应用自定义 FAQ	84
71.1 导入自定义应用的规格？	84
71.2 自定义应用可以用任意的端口号吗？	84
71.3 自定义应用选择规则都必须填写吗？	84
71.4 会话监控里用户和应用没有被识别？	84
72 中英文切换 FAQ	84
72.1 为什么切换成英文版系统日志和操作日志会显示中文日志？	84
72.2 切换成英文版的设备控件显示中文？	84
72.3 切换中英文版本会导致配置丢失吗？	84
73 用户标签 FAQ	85
73.1 用户标签使用前置条件	85
73.2 标签上报服务器规格	85

73.3 标签规格	85
73.4 设备记录用户标签规格	85
73.5 用户标签使用场景	85
73.6 用户标签上报类型	85
73.7 用户标签存储周期	85
73.8 用户标签上报周期	85
73.9 日志上报失败的条件	86
73.10 日志上报标签错误或者无记录排查	86
73.11 用户标签启用禁用	86
73.12 用户标签 ID 对应关系	86
74 AD 域单点登录 FAQ	88
74.1 AD 域单点登录仅支持单域	88
74.2 关于 AD 域单点登录启动脚本	88
74.3 关于 AD 域单点登录数据	88
74.4 AD 域单点登录不支持 HA 同步?	88
74.5 不同用户登录同一台域内测试 pc, 在线用户只显示一个账号?	89
75 服务器负载均衡 FAQ	89
75.1 服务器负载均衡算法	89
75.2 权重大小的说明	89
75.3 探测方式说明	89
76 限额策略 FAQ	89
76.1 限额策略支持流量限额	89
76.2 限额策略支持时间限额	89
76.3 限额策略惩罚方式	90
76.4 惩罚通道的配置	90
76.5 流量限额提醒功能对 https 页面访问是否生效?	90
76.6 建立多条限额策略,但是同一个用户只能匹配最上面的一条策略,其余策略无法匹配?	90
77 无线非经 FAQ	90
77.1 升级最新非经版本之后, ACG 设备上为什么没有无线非经模块	90
77.2 开启无线非经功能之后, ACG 设备上没有任何审计日志	90
77.3 ACG 设备上收到了 Radius 报文,但是并未审计到 Radius 相关账号信息导致非经日志不产生	90
77.4 开启无线非经功能之后, ACG 设备本地有审计日志,但是未产生非经日志	90
77.5 ACG 设备本地产生了非经日志,但是网监平台反馈未收到	91
77.6 网监平台反馈上报的上网数据为什么都来自同一个 AP	91
77.7 网监平台反馈某些应用日志的账号为真实身份账号,非虚拟身份账号	91
77.8 AP 配置导入时, AP 导入文件中不能在一个 AP 上配置多个 AP 地址范围进行导入	91

78 WEB 页面提示格式化硬盘	91
78.1 Web 页面提示格式化硬盘的条件.....	91
78.2 Web 页面格式化硬盘后，设备的状态	91
78.3 设备启动后，硬盘没有挂载成功？	92
78.4 设备启动后，硬盘没有识别，UI 上不显示硬盘？	92
79 接口及其他 FAQ	92
79.1 使用 40GE 的 1 分 4 线缆，ACG1000-X1 的 8 个 10GE 口接上后，接口识别 ERROR，最后两个 10GE 口不 UP？	92
79.2 接口从地址是否能配置为相同网段？	92
79.3 设备编码格式是什么？	92

1 部署方式 FAQ

1.1 ACG应部署在哪里？

ACG 推荐使用在某个区域的网关或与外网接入处，一般来说，外部网络是最具有威胁的。当所有外网流量进入内网时都需要经过边界网关。由此来说 ACG 放置的最佳位置应为与外网接入的地方。如果内网某一区域对安全性有要求也可放置 ACG。但要注意，所有 ACG 应放在区域与区域相接处。

1.2 ACG部署方式有哪些？

ACG 能够工作在三种模式下：路由模式、透明模式和旁路模式。如果 ACG 以第三层对外连接（接口具有 IP 地址），则认为 ACG 工作在路由模式下；若 ACG 通过第二层对外连接（接口无 IP 地址），则 ACG 工作在透明模式下；若 ACG 在完全不影响原网络运行的情况下部署，则 ACG 工作在旁路模式下。

1.3 什么是路由模式？

当 ACG 位于内部网络和外部网络之间时，需要将 ACG 与内部网络、外部网络区域相连的接口分别配置成不同网段的 IP 地址，重新规划原有的网络拓扑，此时相当于一台路由器。也就是说，路由模式 ACG 连接两个不同的子网。

1.4 路由模式使用在什么情况下？

在网络出口需要定义一些访问控制列表（ACL）来对内外网访问进行更严格的要求时，采用路由模式时，路由模式 ACG 可以完成 ACL 包过滤、NAT 转换等功能。

1.5 路由模式下无法访问外网？

如出现该情况可检查路由表，执行 **display ip route** 命令查看路由表中是否存在外网路由，如路由表正常，查看 ACG 安全策略，在 ACG 设备中默认安全策略为 **deny**，需要手工设定放行条目，执行 **display running-config policy** 命令查看 ACG 安全策略。

1.6 什么是透明模式？

透明模式 ACG 进行工作时，可以避免改变拓扑结构造成的麻烦，此时 ACG 对于子网用户和路由器来说是完全透明的。也就是说，用户完全感觉不到 ACG 的存在。

1.7 透明模式无效果？

检查物理接口是否划入到了 bvi 接口中，**display running-config interface** 查看当前接口下信息。

1.8 透明模式的工作原理？

在透明模式下，ACG 将流过的所有二层数据进行解封装，把数据根据用户定义的规则进行从二层到四层的过滤。但与路由模式不同的是，ACG 会将过滤后的数据重新用原来的二层源地址和目的地址再封装成帧进行转发，而不改变数据帧的源地址和目的地址。

1.9 透明模式的实用性在哪里？

透明模式 ACG 一般使用在原网络拓扑在已经完善的情况下增添 ACG。配置透明模式 ACG，ACG 相当于二层设备。可以将 ACG 的多个接口连接到相同子网。可以在不更改其他设备的路由网关对网络进行保护。减少工作量。

1.10 什么是旁路模式？

旁路模式在不更改原网络部署环境的前提下使用。旁路模式 ACG 将通过的流量进行监听、审计等作用。

1.11 使用旁路模式的好处是什么？

旁路模式部署不会大范围影响原网络拓扑结构。只需在原出口设备连接上 ACG 即可。

1.12 查看ACG日志信息为空时怎么处理？

查看旁路模式 ACG 审计日志时无相应显示，该情况可查看策略配置，执行 **display running-config policy** 命令于查看 ACG 的部署策略。

1.13 部署ACG有什么好处？

ACG 具有很好的保护网络安全的效果。入侵者必须首先穿越 ACG 的安全防线，才能接触目标计算机。用户可以将 ACG 配置多种策略，如控制端口、协议、应用等。

1.14 为什么ACG配置正确但是数据无法通过？

ACG 默认存在一条全拒绝的控制策略，使用 ACG 时应先注意安全策略是否匹配。

2 设备管理 FAQ

2.1 为什么管理员用户不能通过HTTP、SSH、或者Telnet登录设备，不显示web页面？

确认登录的接口是否允许通过这些方式登录，可以在每个接口下进行具体配置，详细配置请参见命令行配置指导或者 Web 配置指导。

2.2 为什么HTTPS无法打开防火墙的WEB页面？

查看接口下是否配置了 HTTPS 访问控制，查看是否开启了管理员证书认证功能但并没有对应的证书。

2.3 在“系统管理>管理员”，“添加管理员”页面中的"管理IP/掩码"的作用是什么？

可在"管理 IP/掩码"输入框中以"IP/掩码"的形式设置用户主机的 IP 和掩码，用户登录时，如果用户名、密码正确，并且用户的主机地址与其设置的任意一组 IP 和掩码与运算的值相等，就可以成功登录。如果用户没有设置"管理 IP/掩码"或任意一组"管理 IP/掩码"设置为"0.0.0.0/0"，则登录时不会判断用户的主机地址，只要用户名、密码正确既可成功登录。

2.4 用户登录成功后，可在哪里修改密码？

在“系统管理>管理员”页面中，点击某管理员的<编辑>按钮，进入“修改管理员”页面，即可修改该管理员的密码。也可以点击页面上方右侧的“修改密码”图标，进入“修改密码”页面，即可修改当前登录用户的密码。

2.5 默认admin管理员账户的密码如何重置？

断电或 reboot 重启设备，按 ctrl+c 进入 menuboot，当出现 “Please input your choice[0-8]:” 时，输入'4',执行 **Reset administrator passowrd** 并输入'0'重启设备，重启后，密码即可恢复为默认的 admin/admin 登录。

2.6 什么是管理员双因子认证？

结合管理员登录账号和 Ukey 证书双重身份的认证方式。

2.7 USBkey支持哪些厂商？

USBKey 目前仅支持 epass 一个厂商。

2.8 更新CA根证书后https访问设备不能打开设备登录界面？

在管理员双因子认证功能已正常开启的情况下，如果设备 CA 证书发生变更，需要先关闭管理员双因子认证功能然后再次开启，以便重新关联新的 CA 根证书。

2.9 使用IE浏览器https无法访问设备WEB界面？

IE 浏览器因对证书安全检验级别较高，不受信任的证书网站浏览器会禁止用户继续访问，导致无法通过 https 访问设备。

2.10 火狐浏览器默认不能调用Ukey中的证书？

火狐浏览器需要做兼容性设置，否则无法调用 Ukey 中的证书，设置方法参见后面第 5 节：火狐浏览器兼容性设置方法。

3 应用审计 FAQ

3.1 如何查看当前的应用审计策略？

可以使用命令 **display running poliy** 查看当前的应用审计策略。

3.2 应用审计可以做关键字过滤吗？

通过配置应用审计策略，可以实现关键过滤。

3.3 应用审计日志可以存储多少条？

当日志占用空间超过硬盘容量 95%时就会删除日志，直到日志占用空间为 85%时停止删除。

3.4 应用审计日志按照时间查询多天日志时，为什么会有空白页？

日志查询结果按天显示，如果某一天没有所要查询的日志，那么该天对应的日志查询结果页面为空。

3.5 为什么应用审计不报日志？

- (1) 首先检查应用审计策略是否正确；
- (2) 查看应用审计日志是否记录；
- (3) 查看应用审计与识别的细节信息，判断是否识别与审计成功；
- (4) 通过查看首页应用流量排名统计来查看是否有误识别和漏识别情况；
- (5) 查看特定 IP 地址的会话的 AppName 字段来确认是否为误识别，命令为：**display ip connection protocol protocol-name ip source source-addr dest dest-addr**；调试命令：**debug app audit detail, debug application identify**。

3.6 为什么访问网站未记录网站访问日志？

- (1) 检查应用审计策略是否正确；
- (2) 查看应用识别审计是否开启；
- (3) 所访问网站是否符合包含 content-type 字段类型为 text/html；
- (4) 查看 HTTP 返回码是否为 200；
- (5) 查看网页标题长度是否大于 128 字符；
- (6) 查看 URL 长度是否大于 512。

3.7 为什么恶意URL白名单不生效？

恶意 url 白名单是精确匹配。例：被阻断的网站为 qq.com，新建恶意 URL 白名单 www.qq.com 后还是不能访问，只能是 qq.com，才能访问。

3.8 为什么远程syslog服务器收不到日志？

- (1) 查看应用审计日志是否发送，日志服务器是否启用，服务器 IP 及端口是否正确；
- (2) Syslog 服务器是否启动，端口是否与设备配置一致；
- (3) 查看路由是否正确，ping 服务器地址是否能 ping 通。

3.9 邮件日志中为何有的邮件日志对应的是下载按钮，有的邮件日志对应的是查看按钮？

使用邮件客户端，配置不加密，审计到的邮件日志对应的是下载按钮；webmail：新浪邮箱、QQ 邮箱等，审计到的邮件日志对应的是查看按钮。

3.10 为何邮件日志中有时看不到查看的按钮？

达到了邮件还原的最大限制数。

4 用户信息中心 FAQ

4.1 当用户中心用户识别错误的时候，同时用户数已经达到了用户中心的规格数，如何操作？

Clear ucc user 可以清除内存中的用户缓存，清除后便可以识别出新用户。

4.2 为何用户中心的应用日志数有时会多于日志链接的日志页面的总数？

当产生日志时，用户中心的日志计数即加 1，但若使用测试仪，1s 的日志量很大，已经达到了数据库入库的限制，日志在入库时会产生丢失日志的现象，此时便会出现用户中心的日志数少于链接过去的日志数。

4.3 当用户很大时，特定用户的信息为何没有更新？

未到更新时间，用户根据设备型号不同，同步的时间也各不相同，当用户中心规格高于或等于 2w 时，每 15s 同步 250 个用户；低于 2w 时，每 30s 同步 100 个用户。display capacity 命令可以查看当前用户中心的规格数 UCC_USER 即代表的用户中心的用户数，此规格限制是针对内存中对于用户的限制。

4.4 当用户流量很大时，特定用户的审计日志统计信息统计为0？

用户根据设备型号不同，同步的时间也各不相同，当用户中心规格高于或等于 2w 时，每 15s 同步 250 个用户；低于 2w 时，每 30s 同步 100 个用户。并且当在线用户远远大于用户信息中心规格时，超过规格的用户审计日志不会入库，就会出现统计为 0 的情况，**display capacity** 命令可以查看当前用户中心的规格数 UCC_USER 即代表的用户中心的用户数，此规格限制是针对内存中对于用户的限制。

4.5 当用户数量很大时，停流40分钟后CPU0仍然很忙，显示为100%？

系统启动时会创建一个进程 **dplane_email_dump** 专门用来将用户的数据存储到硬盘和数据库中；每隔 30s 就会将用户的数据通过 **update** 语句更新到数据库中，每次最多更新 250 个用户，每个用户每次只有一条数据，更新完该用户的数据后，会将该用户移到链表的尾部，等待下次更新；停流后，用户的数据依然在链表上，没有存储到数据库，设备用户中心最多存储 20000（不同设备型号规格不一样）个用户，每 30s 存储 250 个用户，20000 个用户则需要 40 分钟；

4.6 为何用户流量统计有时会出现某应用类的应用未显示在饼图中？

用户流量统计饼图是显示的 top9 和 9+，9+表示的是除 top9 以外的应用流量统一为其他。但当某应用类的流量小于总流量的 0.8%时，饼图不单独呈现该应用类，只是放在其他里统一呈现。

4.7 为何网站访问分析总数有时会比该用户网站日志总数少？

用户中心网站访问分析中不记录 URL 为其他类的日志数，所以用户中心中的网站访问日志数会比该用户总的网站数少。

4.8 为何用户在线时长有时会比在线用户显示的时长少？

用户中心的在线时长是记录 1 天的总的时间，当跨天的时候，用户中心会重新计算。而在线用户跨天存在时，在线用户所记录的在线时长是总的时间，所以会多于用户中心所记录的在线时长。

4.9 为何用户中心在线时长有时会比在线用户显示的时长多？

设备当天出现重启现象，在线用户会重新识别，重新记录在线时长，而用户中心会把重启前的时间也记录，所以这种情况会出现用户中心的在线时长多于在线用户显示的时长。

4.10 用户中心用户的排名是按照什么方式？

用户中心用户的排名是根据虚拟身份、日志数、流量大小、网站访问数做的综合分析，得到一个权值，按这个值进行的排名。

4.11 为何用户的应用行为不能记录到时间？

时间轴记录的应用行为以及相同应用再次记录的时间间隔如下：

- 即时通讯类登录行为：时间间隔为 1 天，也就是 1 天内时间轴上只会记录不同即时通讯应用。
- 搜索类搜索行为：时间间隔为 2 分钟。
- 社区类发表行为：时间间隔为 1 分钟。
- 邮件类发送行为：时间间隔为 1 分钟。
- 视频类下载行为：时间间隔为 30 分钟。
- 文件传输类文件传输行为：时间间隔为 150 秒。
- 电子商务类搜索行为：时间间隔为 150 秒。

当时间间隔未达到时，同种应用行为不会被记录到时间轴上。

4.12 为何在无线环境下在用户中心看到的账号信息不正确？

由于无线网络时多个用户同时使用无线，使得用户中心看到的账号信息为多个用户所使用的账号信息，不建议在无线下使用用户中心查看用户信息，仅做参考使用。

4.13 为什么用户信息中心只记录部分审计日志计数后不入库了？

数据中心数据统计入库存在保护机制。当设备最后一个核 CPU 的使用率大于 90% 时，将不在进行数据更新入库操作，统计流程进入保护状态。当设备最后一个核 CPU 的使用率降低至小于 60% 时，统计流程恢复，正常记录更新数据统计入库。

5 流控 FAQ

5.1 带宽的上下行如何区分？

从线路策略绑定接口出去的流量为上行，从线路策略绑定接口进来的流量为下行。

5.2 配置最大带宽和保障带宽为何无法成功？

流量控制通道的保障带宽必须小于等于其最大带宽，流量控制通道的保障带宽必须小于等于其上一级通道的保障带宽。流量控制通道的最大带宽必须小于等于其上一级通道的最大带宽。

5.3 流量控制通道有多个匹配条件时如何匹配？

多个匹配条件是与的关系，当同时满足所有匹配条件时才认为命中该通道。当一个流控通道的匹配条件为空时，会去匹配其子节点的匹配条件。

5.4 最大带宽和保障带宽分别有什么作用？

最大带宽只是起到一个限制的作用，限制流量不能超过其最大带宽。保障带宽的作用是在流量发生拥塞的时流量仍能够达到其保障带宽。

5.5 配置了保障带宽但是在拥塞时流量无法达到其保障带宽？

需要检查如下配置是否正确：

- (1) 线路的最大带宽和保障带宽和其实的带宽一致，若外网的带宽为 20M，就需要配置线路的最大带宽和保障带宽为 20M。
- (2) 下一级通道的保障带宽总和（包括缺省通道）是否已经超过了其保障带宽。

5.6 配置了多个流量控制通道，只有第一个通道有流量匹配？

多个流量控制通道是按顺序匹配的，若流量和某一条流量控制通道匹配，就不会再匹配后续的流量控制通道。

5.7 什么是流量排除策略？

QOS 排除策略也称为白名单，就是指定的用户或者地址的流量，不受 QOS 管制，直接转发，最大限度的保证这些用户使用网络。

5.8 每IP限速和通道带宽限制的处理关系？

流量先被每 IP 限速处理，然后再被流控通道处理。每 IP 限速的周期是一秒，流控通道是实时的。被 IP 限速通过的流量可能会继续被流控通道丢弃。

5.9 如何限制P2P的流量？

P2P 的流量存在不对称性，可能会出现大量的下行流量。多余的流量被流控通道丢弃，但是会影响总体的带宽使用率；建议在实际部署时减小 P2P 的上行流量，这样可以有效抑制下行流量。

5.10 流量控制通道的高、中、低级别有何作用？

当发生带宽借用时，高级别的通道优先借用带宽。若多个通道的级别相同，则平均分配借用带宽。

5.11 子通道的保障带宽总和大于父通道保障带宽，如何分配保障带宽？

当子通道的保障带宽之和大于父通道，按照各个子通道的保障带宽比例分配。

5.12 线路整体带宽仍然有富裕，部分应用延时很大？

对延时要求高的一类应用可以放在单独的流控通道中，该通道的流量不要超过其保障带宽。
查看当前通道流量的命令 **display qos statistics**。

5.13 QOS通道带宽自适应？

Qos 通道带宽自适应，只支持 WEB 页面配置，不支持命令行配置。

5.14 QOS通道带宽百分比范围？

限速百分比支持 0.01-100%，并且支持 4 位有效数字，所有小于 0.01 的都显示为 0.00%。

5.15 QOS通道带宽联动？

- (1) 配置限速通道的保障带宽、最大带宽的限速百分比；自动根据父通道的保障带宽、最大带宽、当前通道的保障带宽生成绝对速率。
- (2) 配置限速通道的保障带宽、最大带宽的限速速率；自动根据父通道的保障带宽、最大带宽、当前通道的保障带宽生成百分比。
- (3) 更改父线路或者父通道的保障带宽、最大带宽、子通道的最大带宽、保障带宽自动根据百分比发生变化。

5.16 QOS通道自适应算法说明

- (1) 初次配置的带宽百分比是基数不会变。
- (2) 用带宽/线路值=百分比 A（如果 $\geq 8Kb$ 显示正常的带宽；算出来的带宽 $< 8kb$ ，带宽置为 8kb，百分比 A 不变（带宽最小 8kb））。
- (3) 调整线路后，用百分比 A*调整后的线路=带宽值。如果 $\geq 8Kb$ 显示正常的带宽；算出来的带宽 $< 8kb$ ，带宽置为 8kb，百分比 A 不变（带宽最小 8kb）。
- (4) web 页面 qos 通道页面编辑后提交。相当于带宽重新下发，需要以 web 页面当前的带宽和线路算百分比。

5.17 QOS通道自适应每IP和每用户说明

- (1) ui 先配置带宽后配置每 ip 的时候有检测，命令行配置 perip 带宽不检测。
- (2) 如果上一步的基础上修改线路带宽后，页面不做检测，修改线路带宽不受影响。
- (3) ui 修改通道带宽或者编辑通道的时候，UI 会检测 perip 大于通道最大带宽，弹出提示。
- (4) 这种情况如果保存配置重启，配置不会丢失。

5.18 QOS透明部署配置Qos时，线路绑定说明

在透明部署模式下配置 QoS 时，线路中绑定的接口必须是 bvi 接口的成员物理接口，功能才能生效，若在线路中绑定 bvi 接口则 QoS 功能无法生效。

5.19 QOS三层部署配置Qos时，线路绑定说明

在三层部署模式下进行 QoS 时，线路中绑定的接口必须是三层接口，功能才能生效。另外，当使用 bvi 接口进行三层转发时，QoS 线路需要绑定在 bvi 接口上才能生效。

5.20 QOS子接口部署配置Qos时，线路绑定说明

在子接口模式下进行 QoS 时，线路中绑定的接口必须在子接口上做，绑定在子接口的物理口上不生效。

5.21 QOS聚合接口部署配置Qos时，线路绑定说明

在聚合接口模式下进行 QoS 时，线路中绑定的接口必须在聚合接口上做，绑定在聚合接口的物理口上不生效。

5.22 如何定位QoS策略是否被命中，命中哪条QoS策略？

可在命令行下执行 “**debug qos match**”，通过 debug 消息可知道具体命中条目。

5.23 如何定位数据包是否被QoS策略丢弃？

可在命令行下执行 “**debug qos drop**”，通过 debug 消息可知道数据包是否被 QoS 丢弃。

6 设备流量统计 FAQ

6.1 设备流量统计的值为何比实际数据包的速率小？

设备流量统计收发包的大小实际上是去掉了 4 字节的 CRC 校验，所以会小于实际的流速。使用实际的发包大小减去 4 字节，再计算出来的流速将与设备统计值相等。

设备整机转发流量中上行、下行如何区分？

整机转发流量统计的为设备的流速，上行即为外网口的发包速率，下行即为内网口的发包速率。当不设置外网口时，上行流速即为 0。

6.2 设备流量统计为何与用户流量统计有所出入？

设备整机流量统计本地发包和转发，而用户流量统计只统计转发的流量，所以两者的值会有所出入。

6.3 设备异常掉电后，为何丢失了部分数据？

设备流量统计的值每隔 1 小时会把数据保存一次，当设备异常掉电，未能及时保存数据，设备启动后，最多会丢失 1 小时的数据。

6.4 更改系统时间对设备流量统计会产生哪些影响？

设备流量统计，每次取的时间是绝对时间。更改系统时间，设备流量统计不会随着系统时间的更改而变化。当设备时间为 10: 00，已经产生近一小时的流量图，把系统时间更改为 11: 00 时，近一小时的流量图依然不变，只是显示的时间有所更改，变为 10: 00-11: 00 的流量图。同理当更改为 9: 00 时，设备流量图依然不变，显示的时间变为 8: 00-9: 00。

特殊情况是：当更改完系统时间后马上重启，此时会对设备流量图有所影响。

如上的例子，当设备时间为 10: 00，更改为 11: 00 后，马上重启，启动后设备流量图 10: 00-11: 00 会为 0，之前的数据依然保存。当更改为 9: 00，马上重启，启动后，9: 00 之前的数据会为空，因为更改时间后，把之前的数据给覆盖了，所以之前的数据都会为空。

6.5 接口状态页面，没有完全显示所有接口的状态信息？

接口状态页面显示的接口信息是物理接口的接口信息，不包括子接口、网桥接口、聚合接口、隧道接口和 3G 接口的状态信息。

6.6 接口状态页面上有接收或发送速率的信息，但健康统计页面整机转发流量无数据？

接口统计的数据为接口接收到或转发的流量信息，而整机转发的流量是指结果设备处理的流量信息，如果接口接收到或转发的流量没有经过设备处理，则整机转发流量信息为空。

6.7 设备健康统计页面，整机转发流量只能看到上行或者下行的流量信息？

整机转发流量的上行流量和下行流量，是通过接口的内网口和外网口属性来确定的，通过内网口转发的流量为下行流量，通过外网口转发的流量为上行流量。

6.8 接口状态页面的数据，多长时间更新一次？

接口状态页面的数据，默认自动刷新的时间为 30s，也可以手动刷新，刷新时向后台获取一次数据。

7 策略路由 FAQ

7.1 什么是策略路由？

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

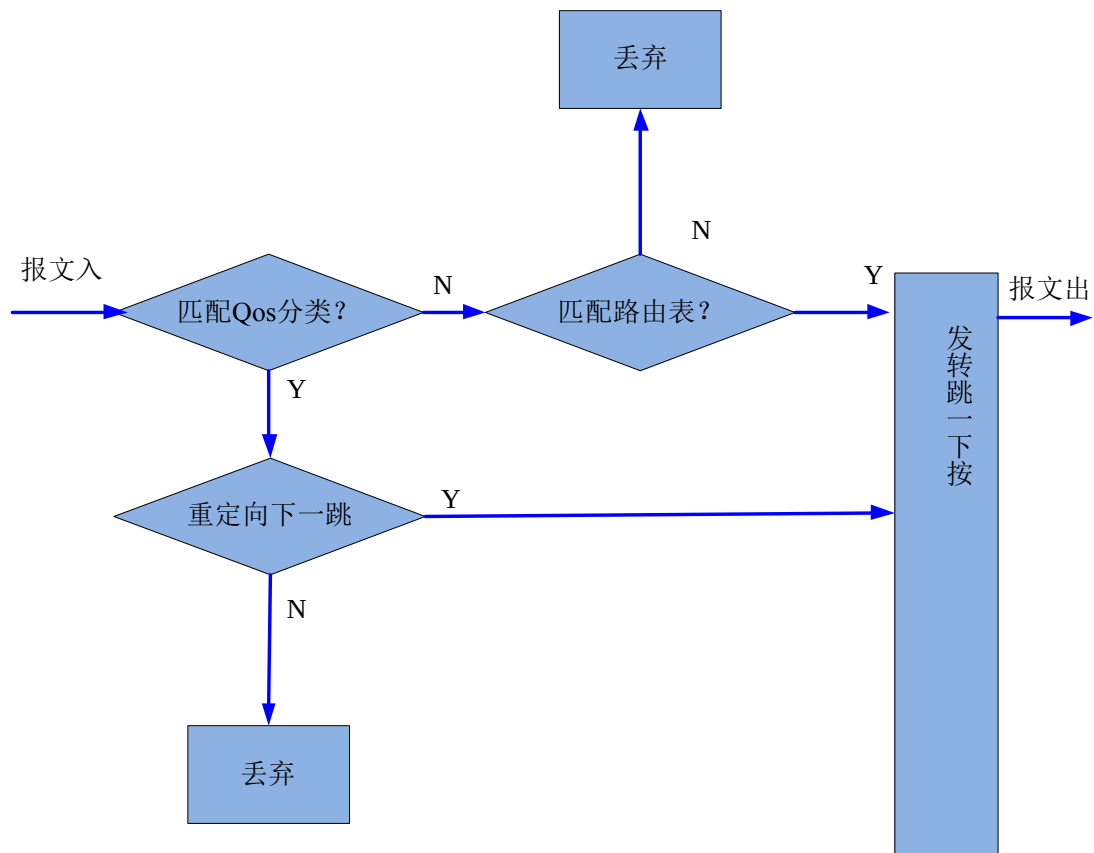
7.2 同一条策略路由最多支持几个下一跳？同时配置多个下一跳的情况下，如何转发报文？

目前，设备支持同一条策略路由中配置 8 个不同下一跳。

同一条策略路由中同时配置多个下一跳的情况下，第一个下一跳作为主用路由，其余下一跳作为备份路由，实现路由备份功能。

7.3 策略路由转发流程图

图7-1 策略路由转发流程图



7.4 策略路由下一跳不可达的判断条件是什么？

通常我们都认为下一跳失效的判断条件为下一跳是否可达，但实际上设备在实现上并没有探测下一跳是否可达的机制，因此设备只能根据自身的各种因素进行判断。下面我们分两种情况进行讨论。

(1) 下一跳是直连网段地址的情况：

设备判断下一跳是否可达的条件是 ARP，只要存在正确的对应下一跳地址的 ARP 表项，则策略路由认为下一跳可达。值得一提的是，如果配置静态 ARP，则需要同时配置对应 VLAN 和出接口，此时策略路由才认为下一跳可达。

(2) 下一跳是非直连网段地址的情况：

对于非直连网段的下一跳地址，设备可以进行路由迭代，即针对下一跳地址查找路由表，如果能匹配到路由，则认为策略路由下一跳可达。如果没有匹配到任何路由，或者只能匹配缺省路由，则认为策略路由下一跳不可达。

8 ISP 路由 FAQ

8.1 什么是ISP路由？

ISP 路由是将数据包从一个网络转发到另一个网络中的目的地址的过程。路由器是处在两个网络之间转发数据包的设备。路由器根据路由表中储存的各种传输路径传输数据包，每一个传输路径即为一个路由条目。

8.2 ISP路由的工作环境是什么？

很多用户通常会申请多条线路进行流量负载均衡。然而，一般的均衡是不会根据流量的流向做均衡的，如果网通的服务器通过电信访问，网速就会很慢。安全网关针对该问题，提供 ISP 路由功能，使不同 ISP 流量走专有路由，从而提高网络访问速度。

8.3 ISP路由是怎样工作的？

用户首先需要将内网用户添加到相同的地址对象中，通过引用设置的地址对象，进行配置不同运营商为目的地的 ISP 路由。用户可以自定义 ISP 信息，也可以上传 ISP 或包含不同 ISP 信息的配置文件。

8.4 ISP路由如何进行流量负载均衡？

ISP 路由在 NAT 配置、安全策略配置时可直接调用相应地址对象的流量。通过 ISP 路由策略（双 ISP 缺省路由）进行控制相应的流量走向问题，从而达到负载均衡。

8.5 ISP路由和静态路由有什么区别？

- (1) ISP 路由下发的就是静态路由，只不过 ISP 路由支持以文件的形式批量下发路由，为了便于区分两种路由的下发形式，**display ip route** 中在手工配置的静态路由前会标识 S，ISP 形式下发的路由前会标识为 I。
- (2) ISP 路由下发的条目在静态路由配置页面不显示，进行了过滤，避免影响用户手工创建的静态路由的配置查看。
- (3) 静态路由和 ISP 路由规格是共用的，是占用的同一个规格表。
- (4) 如果配置一条静态路由再自定义创建一条 ISP 路由分别指向不同的下一跳，实现的是等价路由的效果
- (5) 存在 ISP 路由的情况下，再创建相同的静态路由，静态路由不能下发，实际还是一条路由，反之亦然。
- (6) CLI 下通过 **no ip route xxxx** 可以删除相应的 ISP 路由，如果要恢复此条 ISP 路由，需要删除 ISP 路由重新创建以触发下发整个 ISP 路由表。

9 IPsec VPN FAQ

9.1 如何查看当前IKE SA信息？

可以使用命令 **display ike sa** 查看当前 IKE SA 的信息：

```
HOST# display ike sa
-----
Name: dut1      id: 3184
    local_addr: 30.1.1.2
    peer_addr: 30.1.1.3
    stat: establish
    life time: 86390
*****
Data: ike sa    Total count: 1.
*****
```

9.2 如何查看当前IPsec sa信息？

可以使用命令 **display ipsec sa** 查看当前 IPsec sa 的信息。

```
HOST# display ipsec sa
-----
Name: dut1      id: 4667
    local_addr: 30.1.1.2    peer_addr: 30.1.1.3
    esp: yes    mode: tunnel
        enc_algo/auth_algo: aes256/sha1
        inbound_spi/outbound_spi: 237441483/134485286
    ah: no
    stat: establish
    life time/cur_life_time: 86400/86304
    inbound/outbound: 5/5 kbytes
    local_net: 20.1.1.0/24
    peer_net: 10.1.1.0/24
*****
Data: ipsec sa  Total count: 1.
*****
```

9.3 IPsec VPN中报文的默认加密方式是什么？

IPsec VPN 的默认加密方式是 aes256-sha1。

9.4 一条VPN最多支持多少条隧道？

一条 IPsec VPN 隧道，配置多个网段的感兴趣流，最多支持 100 条。

9.5 为什么IPsec VPN第一阶段协商不成功？

- (1) 第一阶段协商不成功，首先可以检查 IKE 的配置，查看两端的配置是否一致。
- (2) 其次检查路由，查看对端是否可达。
- (3) 如果一端配置对端网关配置的是动态，另一端配置静态对端网关，查看配置静态对端网关的一端，是否开启了自动连接，若未配置自动连接，流量需要从静态那一端发起，触发 IKE SA 的协商。
- (4) 一阶段是否配置了两套一样的 IKE 提议：对端 IP，算法提议，对端 ID，本地源 IP，这些信息一样。如果存在两套一样的提议，设备就无法确认使用哪个 IKE 配置进行协商了

主模式：对端 IP，算法提议，本地源 IP（如果配置了就检查）

野蛮模式：对端 ID、算法提议、本地源 IP

无论哪种模式匹配的标准是一样的，对端 IP，算法提议，本地源 IP，对端 ID。只不过如果没有带的话，这一项就不检查了。

调试命令：**debug ipsec-VPN debug**。

9.6 为什么IPsec VPN第二阶段协商不成功？

- (1) 首先可以检查 IPsec 的配置，查看两端的配置是否一致。
- (2) 检测感兴趣流，查看两端的感兴趣流是否一致。
- (3) 检测路由，查看对端是否可达。若是基于 tunnel 口，检查是否配置 tunnel 口的路由。

调试命令：**debug ipsec-vpn debug**。

9.7 为什么保护子网不能通讯？

隧道模式时查看是否配置策略。

查看感兴趣流的方向性是否正确。

若是感兴趣流的问题，可以通过以下命令查看：

display ike dump-tunn，查看基于 tunnel 的 IPsec VPN 的 sp 状态是否建立成功。

9.8 为什么某些移动终端接入VPN不成功？

- (1) 有些手机的 IKE 协商模式是野蛮模式，有些是主模式，所以一条 VPN 隧道不能保证所有的手机都能接入成功。
- (2) 手机发起的加密算法也各不相同，可以通过 **debug ipsec-vpn debug** 命令，查看协商不成功的原因，同时也可以查看对端发来的加密算法是否与本端一致。

9.9 NAT环境下IPSEC协商不成功？

搭建 IPSEC 的环境中间有过 NAT 并且配置了 AH 认证导致 ipsec 无法协商成功，AH 封装的校验从 IP 头开始，如果 NAT 将 IP 的头部改动，AH 的校验就会失败，因此我们得出结论，AH 是无法与 NAT 共存的。此时去掉 AH 认证 IPSEC 可以协商成功。

9.10 IPSEC建起连接后，一端断开后，IPSEC无法协商？

IPSEC 断开后对端设备并没有把原先建立好的 SA 清除，就不再接受再次发起的协商请求，导致无法建立连接。

- (1) 在对端设备手动删除 SA。
- (2) 双方启用 DPD 检测。

9.11 本端SA状态显示连接，流量无法转发？

问题原因：对端手动清除了 SA；对端同时启用了按秒计时和按流量统计，本端只配置了按秒计时，如果流量过大，可能导致在按秒计时的生存周期内流量已经超出，导致对端 SA 端口连接

- (1) 双方把各自一阶段的 SA 生存期和二阶段 SA 生存周期改成一致；
- (2) 一阶段启用 DPD 检测。

9.12 当设备存在多出口时，其它参数正确，IPSEC协商失败？

- (1) 当有多出口时，需要指定用于建立 IPsec 的本端 IP 地址。
- (2) 如果指定的是本地源接口，则使用该接口上的主 IP 作为本端 IP 地址。

9.13 IPSEC使用国密证书协商不成功？

- (1) IPSEC 认证方式选择国密认证后，需要填写本端证书、对端证书和 CA 证书。
- (2) 协商不成功需要检查本端证书与对端证书是否导入正确。

9.14 IPSEC快速配置与IPSEC VPN标准配置有什么区别？

- (1) IPSEC 快速配置大大简化了 IPSEC VPN 配置，接入一个新的站点只需要配置节点类型、本端或对端网关 IP，保护网段即可实现 IPSEC 接入，IKE 一阶段、IPSEC 二阶段、tunnel 接口、保护网段路由等动态生成。
- (2) IPSEC 快速配置支持网段映射，能很好的解决分支站点保护网段冲突的情况。
- (3) IPSEC 快速配置支持选路策略动态调整，调整主备链路只需要调整分支节点线路顺序，设备会根据线路顺序自动调整路由优先级，默认线路优先级为 5、6、7、8，最多支持 4 条线路。

9.15 IPSEC快速配置一阶段和二阶段默认参数？

- (1) 执行命令 **display ike easy-ipsec-gen** 可以查看一阶段默认参数如下：

```
set mode main
set remotegw 172.16.1.1
authentication pre-share
lifetime 86400
dpd enable
dpd interval 5
```

```
dpd retry-interval 2
set nat 10
group 2
set policy 1
  encrypt 3des
  hash md5
```

(2) 执行命令 **display ike easy-ipsec-gen** 可以查看二阶段默认参数如下：

```
vpn ipsec phase2
  mode tunnel
  auto-connect enable（分支节点开启自动连接，中心节点默认关闭自动连接）
  auto-connect interval 10
  set lifetime seconds 86400
set proposal1 esp-aes256-sha1 ah-null
```

9.16 IPSEC快速配置默认参数支持修改吗？

IPSEC 快速配置一二阶段默认参数不支持修改，进入命令行编辑模式时会有错误提示，不允许用户修改。

9.17 IPSEC预共享密钥有字符限制么？

预共享密钥尽量避免使用特殊字符，如“<>”否则有可能出现显示报错，但不影响最终使用，尽量避免。

9.18 主链路断开后为什么ipsec链路没断开？

因为每一条 ipsec 链路都有设置的老化时间，链路断开后，会等待 ipsec 链路老化时间结束后，再根据设置的切换时间切换链路。

9.19 主链路被引用后还能继续当做其他链路的备链路吗？

不能，主备链路是一对一的关系，被引用的主链路和备链路都不能再被其他链路引用。

9.20 主备切换必须等待ipsec老化时间结束才能切换吗？

一般情况下，需要等待 ipsec 链路老化时间结束后才开始切换时间，但是可以在 ike 配置 DPD 对端检测，链路断开后，根据设置的对端检测时间，ipsec 链路就会断开。

9.21 主链路选择连接方式为监控链路故障自动连接后主链路选择下拉为什么为空？

主链路选择是指备链路来选择哪条链路作为主链路，主链路配置的时候不需要选择连接方式为监控链路故障自动连接。

9.22 链路断开是监控哪个阶段？

主备链路监控的是 IPSEC SA 的状态。

9.23 使用测试仪打单向流量，一条隧道的情况下为什么解密端cpu0核使用率很高？

目前对于低端设备没有完全意义上的控制核，cpu0 核也会处理 ipsec vpn 业务，数据包通过 ipsec 加密端设备加密后就变成了相同的五元组：协议、源目的 IP、源目的端口的报文，由于设备支持流保序功能，从而导致流量默认全部分到了 cpu0，可通过 `switch keep-order off` 命令关闭。

9.24 IPSEC场景，DPD未开启的情况下，ipsec关联的物理接口down后，ike和ipsec sa不会跟随断开连接？

IPSEC 设置有 3 种：本地源接口，本地源 IP，无，对于本地源 IP 和无的配置，接口 down 是无法判断要清除那个 SA 的，所以统一处理逻辑为接口 down 不自动清 IKE，通过 DPD 机制来检测链路状态即可，DPD 保活失败，会自动清除 SA

10 IPv6 FAQ

10.1 配置IPv6有什么优点？

IPv6 具有 128 位的 IP 地址结构，提供充足的地址空间。层次化的网络结构，提高了路由效率。支持自动配置，即插即用。支持端到端的安全。支持移动特性。新增流标签功能，更利于支持 QoS。

10.2 什么是IPv6邻居发现协议？

邻居发现协议(Neighbor Discovery Protocol)是 IPv6 协议的一个基本的组成部分，它实现了在 IPv4 中的地址解析协议(ARP)、控制报文协议(ICMP)中的路由器发现部分、重定向协议的所有功能，并具有邻居不可达检测机制。

邻居发现协议实现了路由器和前缀发现、地址解析、下一跳地址确定、重定向、邻居不可达检测、重复地址检测等功能。

10.3 IPv6中的路由器请求报文作用（Router Solicitation）？

当主机没有配置单播地址（例如系统刚启动）时，就会发送路由器请求报文。路由器请求报文有助于主机迅速进行自动配置而不必等待 IPv6 路由器的周期性 IPv6 路由器通告报文。

IPv6 路由请求为 ICMP 报文，类型为 133。

IPv6 路由器请求报文中的源地址通常为未指定的 IPv6 地址（0::0）。如果主机已经配置了一个单播地址，则此接口的单播地址可在发送路由器请求报文时作为源地址填充。

IPv6 路由器请求报文中的目的地址是所有路由器组播地址（FF02::2），作用域为本地链路。如果路由器通告是针对路由器请求发出的，则其目的地址为相应路由器请求报文的源地址。

10.4 IPv6中的路由器通告报文作用（Router Advertisement）？

每个 IPv6 路由器的配置接口会周期发送路由器通告报文。在本地链路上收到 IPv6 节点的路由器请求报文后，路由器也会发送路由器通告报文。

IPv6 路由器通告报文发送到所有节点的链路本地组播地址（FF02::1）或发送路由器请求报文节点的 IPv6 单播地址。

路由器通告为 ICMP 报文，类型为 134，包含以下内容：

- 是否使用地址自动配置。
- 标记支持的自动配置类型（无状态或有状态自动配置）。
- 一个或多个本地链路前缀-本地链路上的节点可以使用这些前缀完成地址自动配置。
- 通告的本地链路前缀的生存期。
- 是否发送路由器通告的路由器可作为缺省路由器，如果可以还包括此路由器可作为缺省路由器的时间（用秒表示）。
- 和主机相关的其它信息，如跳数限制，主机发起的报文可以使用的最大 MTU。

10.5 邻居请求（Neighbor Solicitation）报文作用？

当一个节点需要得到同一本地链路上另外一个节点的链路本地地址时，就会发送邻居请求报文。此报文类似于 IPv4 中的 ARP 请求报文，不过使用组播地址而不使用广播，只有被请求节点的最后 24 比特和此组播相同的节点才会收到此报文，减少了广播风暴的可能。

源节点使用目的节点的 IPv6 地址的最右 24 比特形成相应的组播地址，然后在相应链路上发送 ICMPv6 类型为 135 的报文。目的节点在响应报文中填充其链路地址。为了发送邻居请求报文，源节点必须首先知道目的节点的 IPv6 地址。

邻居请求报文也用来在邻居的链路层地址已知时验证邻居的可达性。

10.6 邻居通告（Neighbor Advertisement）报文作用？

IPv6 邻居通告报文是对 IPv6 请求报文的响应。

收到邻居请求报文后，目的节点通过在本链路上发送 ICMPv6 类型为 136 的邻居通告报文进行响应。收到邻居通告后，源节点和目的节点可以进行通信。

当一个节点的本地链路上的链路层地址改变时也会主动发送邻居通告报文。

10.7 邻居发现协议的功能是什么？

- 路由器和前缀发现。
- 地址解析。
- 重定向功能。
- 邻居不可达检测。
- 重复地址检测。

10.8 在配置IPv6静态路由之前，需完成以下任务？

配置相关接口的物理参数，配置相关接口的链路层属性、使能 IPv6 报文转发能力、邻节点网络层（IPv6）可达。

10.9 IPv6缺省路由的生成方式？

IPv6 缺省路由是在路由器没有找到匹配的 IPv6 路由表项时使用的路由。

IPv6 缺省路由有两种生成方式：

- 第一种是网络管理员手工配置。指定的目的地址为::/0（前缀长度为 0）。
- 第二种是动态路由协议生成，由路由能力比较强的路由器将 IPv6 缺省路由发布给其它路由器，其它路由器在自己的路由表里生成指向那台路由器的缺省路由。

10.10 在Tunnel接口上配置了相关的参数后（例如隧道的起点、终点地址和隧道模式）仍未处于up状态？

可以按照如下步骤进行：

- (1) Tunnel 接口未处于 up 状态的最常见原因是隧道起点的物理接口没有处于 up 状态。使用 **display interface** 和 **display ipv6 interface** 命令查看隧道起点的物理接口状态为 up 还是 down。如果物理接口状态是 down，请检查网络连接。
- (2) Tunnel 接口未处于 up 状态的另一个可能的原因是隧道的终点地址不可达。使用 **display ipv6 route** 和 **display ip route** 命令查看是否终点地址通过路由可达。如果路由表中没有保证隧道通讯的路由项，请配置相关路由。

10.11 6to4隧道是否需要配置目的地址？

6to4 隧道不需要配置目的地址，因为隧道的目的地址可以通过 6to4 IPv6 地址中嵌入的 IPv4 地址自动获得。

10.12 ISATAP隧道是否需要配置目的地址？

ISATAP 隧道不需要配置目的地址，因为隧道的目的地址可以通过 ISATAP 地址中嵌入的 IPv4 地址自动获得。

10.13 从设备端执行什么配置去主动ping另一台设备的IPv6地址？

执行 **ping6** IPv6 地址即可，使用 **ping** 命令仅为 IPv4 下使用的。

10.14 什么是IPv6手动隧道？

手动隧道是点到点之间的链路，一条链路就是一个单独的隧道。主要用于边缘路由器—边缘路由器或主机—边缘路由器之间定期安全通信的稳定连接，可实现与远端 IPv6 网络的连接。

10.15 什么是6to4自动隧道？

6to4 隧道是点到多点的自动隧道，主要建立在边缘路由器之间，用于将多个 IPv6 孤岛通过 IPv4 网络连接到 IPv6 网络。6to4 隧道通过在 IPv6 报文的目的地址中嵌入 IPv4 地址，来实现自动获取隧道终点的 IPv4 地址。

6to4 隧道采用特殊的 6to4 地址，其格式为：2002:abcd:efgh:子网号::接口 ID/64，其中 2002 表示固定的 IPv6 地址前缀，abcd:efgh 表示该 6to4 隧道对应的 32 位全球唯一的 IPv4 地址，用 16 进制表示（如 1.1.1.1 可以表示为 0101:0101）。2002:abcd:efgh 之后的部分唯一标识了一个主机在 6to4 网络内的位置。通过这个嵌入的 IPv4 地址可以自动确定隧道的终点，使隧道的建立非常方便。

由于 6to4 地址的 64 位地址前缀中的 16 位子网号可以由用户自定义，前缀中的前 48 位已由固定数值、隧道起点或终点设备的 IPv4 地址确定，使 IPv6 报文通过隧道进行转发成为可能。6to4 隧道可以实现利用 IPv4 网络完成 IPv6 网络的互连，克服了 IPv4 兼容 IPv6 自动隧道使用的局限性。

10.16 什么是ISATAP自动隧道？

现有的 IPv4 网络中将会出现越来越多的 IPv6 主机，ISATAP 隧道技术为这种应用提供了一个较好的解决方案。ISATAP 隧道是点到多点的自动隧道技术，通过在 IPv6 报文的目的地址中嵌入的 IPv4 地址，可以自动获取隧道的终点。

使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的 ISATAP 地址。ISATAP 地址格式为：Prefix(64bit):0:5EFE:abcd:efgh。其中，64 位的 Prefix 为任何合法的 IPv6 单播地址前缀，abcd:efgh 表示 32 位 IPv4 源地址，用 16 进制表示（如 1.1.1.1 可以表示为 0101:0101），该 IPv4 地址不要求全球唯一。通过这个嵌入的 IPv4 地址就可以自动建立隧道，完成 IPv6 报文的传送。

ISATAP 隧道主要用于在 IPv4 网络中 IPv6 路由器—IPv6 路由器、IPv6 主机—IPv6 路由器的连接。

11 VRF FAQ

11.1 不同的VRF间如何相连？

可以通过物理网线相连接，也可以通过虚拟接口如子接口方式相连接。

11.2 ACG1000最多可以创建多少个VRF？

可以创建最多 256 个 vrf，超出时提示：Error: The total number of vrf has exceeded the maximum size(Capacity reached)。

11.3 VRF基本设计概念是什么？

VRF 功能提供了从一台物理路由器变成多台虚拟路由器的功能。ACG1000 的 VRF 功能提供了路由表隔离，接口切换 VRF，外部能够正常支持访问已经切换 VRF 的接口地址，支持本机报文正确选择对应接口向外主动发送报文。

11.4 路由表隔离功能的逻辑？

路由表隔离功能是通过在创建和删除 VRF 时，同时创建对应的 fib 表实现的，实现形式就是每个 VRF 一个独立的 FIB 表，设备在没有开启 VRF 功能时，是默认存在一个 VRF0 结构的，路由表和流表都是从属与该结构。

11.5 流表的隔离功能？

流表的隔离，是通过在流表结构中添加 VRF_ID 字段来实现的，功能主要流程为，在流里结构中添加了一个 VRF_ID 的字段，该 VRF_ID 字段赋值为报文入接口的 VRF_ID，查找流表的时候，比较五元组的同时还需比较 VRF_ID 是否相同，如果五元组和 VRF_ID 均相同，则表示查找成功，否则，新建对应的流表。

11.6 VRF模块设计背景？

VRF 模块属于 ACG1000 的功能模块，实现虚拟路由转发功能。

12 动态路由 FAQ

12.1 RIP支持v1和v2功能吗？

RIP 支持 v1 和 v2 两个版本。

12.2 RIP开启时默认是V1还是V2版本？

RIP 开启时默认为 V2 版本，若需要可以手动切换到 v1 版本。

12.3 OSPF是否支持pppoe接口？

Ospf 不支持 pppoe 接口。

12.4 OSPF的Router ID如何配置，缺省是什么？

简单的说我们采用如下策略：

- 如果有 loopback 接口配置了，就选 IP 地址数值最大的 loopback 地址。
- 如果没有配置 loopback 接口地址，就选 IP 地址数值最大的物理接口地址。
- 选择完成后不可抢占。
- 我们也可以在启动 OSPF 进程时同时指定 Router ID，如：router-id 1.1.1.1。
- 需要注意的是，如果当前 OSPF 进程正在运行，Router ID 即使是重新手工配置或计算都不会马上生效，而需要 OSPF 进程重新启动才会生效。这个要求是合理的，因为 Router ID 对 OSPF 协议来说太重要，不可能在 OSPF 保持邻居不断的情况下更新。

12.5 OSPF没有路由，甚至邻居都不能形成Full关系，最常见的原因是什么？

- OSPF 网络类型是 NBMA 的，但你忘记在 OSPF 协议模式下配置邻居了。
- OSPF 网络类型是 NBMA 的，你配置了邻居，但在诸如 Frame relay 的 map 语句中忘记加 broadcast 关键字了，导致协议报文不能到达对方。
- OSPF 邻居的 hello 及 dead interval 值不一致。
- 在 Stub 或 NSSA 区域，有些路由器没有配置成 Stub 或 NSSA。
- OSPF 验证配置错误。
- OSPF Router ID 有问题，可能和某个其它路由器一样了。
- OSPF 链路两端的网络类型不一致。
- OSPF 链路两端的 MTU 相差比较大，尤其注意和不同厂商实现互通时（需要在其接口下配置 OSPF 忽略 MTU 检查或修改 MTU）。
- 该网络根本就没有启动 OSPF。
- 区域号不一致；链路的网络地址不一致，注意检查两边的 mask。

12.6 有什么好的办法知道OSPF出了什么问题？

其实很简单，也是必须知道的。调试开关是需要打开的，其中最有效，最常用的就是 **debug ospf packet** 命令，协商完成后执行 **display log debug**，它能让你对 OSPF 的大部分问题看的一目了然。当然它也不是万能的，它是在正确接收 OSPF 报文的基础上才能有相应的错误事件。

12.7 OSPF如何自动计算接口cost的？

当链路接口没有明确配置 OSPF cost 的时候，Cost 按配置的基值除以接口带宽来计算。这个基值缺省为 100M，例如 10M 的链路，cost 缺省是 $100/10=10$ 。显然当运行 OSPF 的路由器存在多个速率不同的 1000M 以上的高速接口时候，如果接口没有明确赋予 OSPF Cost，按缺省公式自动计算的 Cost 将都为 1，不能反映链路速率。这个时候有一个 Bandwidth-Reference 的命令，来调节基准值的，但要注意，整个 OSPF 路由域都要对应调整。因此，最好的方法，还是在网络做好规划，手工对链路接口的 Cost 赋值。

12.8 OSPF链路两端配置不同的网络类型，能否形成Full关系？

看起来很奇怪的问题，其实比较有意思。很多人的第一感觉就是：两端的链路网络类型都不一样，哪能形成邻居关系呢？其实不然。OSPF 协议并没有规定，要去严格检查链路的网络类型，链路的网络类型最重要的描述也是在 **Type 1 LSA** 中，形成邻居的关系条件检查并没有去检查它。仔细阅读协议并做实验，你会发现不少情况下，比如两台路由器以太网连接，一端保持缺省的广播网络类型，一端配置成 **OSPF P2P** 网络类型，肯定是可以形成邻居，并交换 **LSDB** 达到 **Full** 状态的。但很奇怪的事情是：到达 **Full** 状态了，为什么学不到路由呢？其实答案很简单，OSPF 路由器需要 **LSDB** 来构建 **SPT** (**Shortest Path Tree**)，由于 **LSDB** 的数据库是脱节的（在我的 **Router LSA** 中，我认为你是个广播邻居；而在你的 **Router LSA** 中认为我应该是 **P2P** 邻居），根本无法构建正确的 **SPT**，**SPF** 算法也无法计算出正确的路由。

12.9 OSPF路由聚合是否可以跨区域聚合？

先看一个问题，简单示意的 OSPF 网络拓扑，**area 1—area0—area2**，**area1** 中三条路由：**10.1.0.0/16**，**10.2.0.0/16**，**10.3.0.0/16**，在 **area1** 和 **area0** 之间的 **ABR** 没有配置聚合（将上述三条聚合成 **10.0.0.0/8**），但在 **area0** 和 **area2** 之间的 **ABR** 配置聚合却不生效。这就是跨区域的聚合问题，这个表现是否正确呢？

仔细看下 **RFC 2328 12.4.3 Summary-LSAs** 中的描述，我们可以知道 **ABR** 产生 **type 3 LSA** 时，如果是 **inter-area**，就直接处理，产生相应的 **type 3 LSA**，而不需要考虑配置的 **range**，而在考虑 **intra-area** 路由的时候，才要去考虑配置的聚合。

所以，上述描述的结果是正常的现象。区域间路由的聚合是在连接产生该路由的区域的 **ABR** 上处理的，而不能跨区域聚合。

12.10 OSPF的Virtual-Link是否很有用处？

从协议的角度上来看，OSPF 的虚连接 **Virtual Link** 非常有用，一是可以将不与骨干区域直接物理连接的区域连接起来，让它能正常路由，这在一些网络的合并中比较有用；二是可以提高网络的可靠性，让骨干区不至于轻易断开而不能正常路由（**RFC 2328** 中的例子）。

12.11 OSPFv3在界面中是否有配置选项？

OSPFv3 仅提供命令行下配置，可以在界面上查看学习到的路由条目。

12.12 OSPFv3邻居无法建立？

如果物理连接和下层协议正常，则检查接口上配置的 **OSPFv3** 参数，必须保证与相邻路由器的参数一致，区域号相同。

相邻的两台路由器接口的网络类型必须一致。若网络类型为广播网，则至少有一个接口的 **DR** 优先级应大于零。

12.13 OSPFv3路由信息不正确？

应保证骨干区域与所有的区域相连接。若一台路由器配置了两个以上的区域，则至少有一个区域应与骨干区域相连。骨干区域不能配置成 Stub 区域。

在 Stub 区域内的路由器不能接收外部 AS 的路由。如果一个区域配置成 Stub 区域，则与这个区域相连的所有路由器都应将此区域配置成 Stub 区域。

12.14 当执行no router ospf6后,其它接口有关ospfv3配置是否自动删除？

各项口下进行的功能特性配置，在删除 router ospf6 主进程后，该接口上的所有配置也将被删除。

13 HA FAQ

13.1 配置HA的优点？

HA 是 High Availability 缩写，即高可用性，可防止网络中由于单个网关产品的设备故障或链路故障导致网络中断，保证网络服务的连续性和安全强度。

随着网络的快速普及和应用的日益深入，各种增值业务（如 IPTV、视频会议等）得到了广泛部署，网络中断可能影响大量业务、造成重大损失。因此，作为业务承载主体的基础网络，其可靠性日益成为受关注的焦点。

在实际网络中，总避免不了各种非技术因素造成的网络故障和服务中断。因此，提高系统容错能力、提高故障恢复速度、降低故障对业务的影响，是提高系统可靠性的有效途径。

13.2 HA的工作模式

目前产品支持两台网关设备以主-备模式运行。

13.3 什么是HA的主备模式？

主备模式是指实现 HA 的两台设备中，一台作为主设备，另外一台作为备设备。主设备在进行业务的同时，将相关的配置和数据信息实时同步到备设备。当主设备出现故障或主设备的链路中断时，备用设备成为主设备，接管原主设备的工作，实现网络业务的无缝切换。

在主备模式下，主设备响应各类报文请求，并且转发网络流量；备用设备不响应报文请求，也不转发网络流量。主备设备之间通过 HA 心跳线同步状态信息，配置信息以及特征库文件。

主备模式支持路由模式和透明模式。

13.4 什么是HA的主主模式？

主主模式是指实现 HA 的两台设备中，两台均为主设备。主设备在进行业务的同时，将流表信息和认证用户信息同步到对端。当其中一台设备出现故障或链路中断时，另外一台设备作为故障设备的备份，接管原主设备的工作，实现网络业务的无缝切换。

在主主模式下，两台设备均工作，转发流量。主主设备之间通过 HA 心跳线同步状态信息。
主主模式支持路由模式和透明模式。

13.5 HA工作状态

HA 主备的工作状态主要有两种，主模式和备模式：

- 主模式是指在设备 HA 主备模式中，实际参与工作。
- 备模式是指设备在 HA 主备模式中，作为主设备备份，不参与实际工作。只有当主设备失效，才转换为主设备，接替其工作。

HA 主主的工作状态为主模式：

- 主模式是指在设备 HA 主主模式中，两台设备均参与工作。其中一台设备出现故障，另外一台承接出现故障的业务。

13.6 HA接口概念

HA 中，主要有两种接口概念：

- HA 接口：连接两台 HA 设备的接口，不参与报文的转发，只用于 HA 设备接收心跳报文和同步报文使用。
- 监控接口：HA 必须重点关注的设备接口，如果此接口状态为 **down**，表明网络状态发生故障，需要切换主备设备来修复故障。

13.7 抢占模式

- 非抢占方式：如果备份组中的路由器工作在非抢占方式下，则只要主路由器没有出现故障，备设备不会主动成为主设备。
- 抢占模式：抢占模式时指用户可以根据需要，制定某一台设备优选为主设备或者为备设备。如果配置优选为主设备的设备工作正常，即使当前设备为备状态，也要“抢占”成主设备。
- HA 的两台设备抢占模式必须匹配。或者全部配置成非抢占模式，或者一个配置成抢占为主，一个配置成抢占为备。否则 HA 无法正确协商。

13.8 抢占延时定时器

为了避免 HA 设备频繁进行主备状态转换，备设备在网络状态恢复为正常状态后，也不会马上抢占为主，而是在流表等信息同步完成后，等待一定时间。只有在这段时间内，设备依然正常，才会通知主设备，抢占成主。

13.9 心跳报文

HA 设备之间用来相互通告设备的 HA 配置和 HA 状态的报文。如果一个设备在规定时间内没有收到邻居心跳报文，可以认定 HA 邻居已经失效。

13.10 HA管理地址

处于备状态的 HA 设备不会参与网络转发，因此无法通过其接口配置的 IP 地址访问。为了解决这一问题，可以在设备上配置管理地址，用作备设备的网络管理。用户可以从外部访问备设备的 telnet 服务和 web 管理界面。

13.11 HA状态同步

HA 作为热备份，为了在状态切换的过程中，尽量减小对网络的影响。HA 会将主设备上的一些实时的状态同步给备设备。同步的内容主要包括三种：session 信息，设备配置，特征库。

- session 信息：包括设备连接表、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 IPS 特征库，AV 特征库，APP 特征库以及 URL 特征库。

13.12 HA主备状态切换

- 当设备启用 HA 主备模式后，设备进入 init（初始化状态）。在这个状态，设备不参与报文转发，只接受对端 HA 设备的 keepalive 报文。如果收到了主设备发出的 keepalive 报文，设备会进入备状态。如果没有收到 keepalive 报文，设备会进入主状态。
- 如果设备成为主状态后，会向外发送免费 arp 报文，用来更新上下游设备的 arp 表（工作在路由模式），或者向外发送特殊的报文刷新上下游交换机的 fdb 信息（工作在透明模式）。
- 如果设备成为备设备，设备会清除自己的 fdb 表（如果工作在透明模式），并且向主设备请求状态信息。

13.13 HA主主状态切换

当设备启用 HA 主主模式后，设备进入 init（初始化状态），然后状态置为 master。设备收到对端发来的 keepalive 报文，两端设备协商参数。建立 master 邻居后，靠心跳报文保持邻居关系，并启动定时器。若在定时器（定时器时间为 interval * retry 次数）时间内，未收到心跳报文，则状态置为 master（A）。出现故障的设备状态置为 master（N）。master（N）状态的设备，监控接口不参与报文转发。

13.14 HA主主邻居为什么建立不起来

- 两台设备必须型号一致，板卡一致。
- 两台设备的序列号要求不一致。序列号一致建不起来邻居。
- 查看心跳线接口状态是否正常。

13.15 HA主主地址代理

两台设备均配置监控接口，当其中一台设备的接口 down 掉后，两台一台设备的接口将对端地址代理，代理地址置为 active，此接口参与出现故障设备的业务转发。

13.16 HA主主非对称路由

Ha 主主环境下，流表信息同步，某种业务的控制报文走的其中一台主主设备，数据报文可以从另外一台设备收上来。

13.17 HA主备场景下执行手动同步配置，备设备重启完成后，主设备HA监控仍显示配置不同？

低端硬件型号不支持硬盘，如果主设备上插了U盘或移动硬盘，而备设备上没有，这样主设备上就会下发非经的配置，备设备由于没有硬盘就不会下发配置的配置，这样就会导致主备手动配置同步后，由于主设备上存在非经的配置，会导致配置对比始终不相同，如果出现此现象，拔掉主设备的U盘重启即可。

14 Bypass FAQ

14.1 每台设备最多有多少组Bypass接口？

根据不同机型分别定义，最少一组 Bypass 接口对，最多不限制。

14.2 Bypass接口使用在哪种网络场景中？

使用在二层网络场景。

14.3 Bypass功能默认开启吗？

Bypass 功能默认开启。

14.4 进程异常时是否会触发Bypass？

系统异常时设备会自动重启，会触发 Bypass。

14.5 系统运行过程断电是否会触发Bypass？

异常断电会触发 Bypass。

14.6 系统启动过程中是否会持续Bypass状态？

会持续 Bypass 状态一直到系统启动成功。

14.7 从系统正常到掉电进入Bypass状态时，会丢几个ICMP报文？

系统断电或启动过程会丢 3 个 ICMP 报文。

15 APP 缓存 FAQ

15.1 APP缓存能缓存哪些文化类型？

可缓存 exe 文件，如缓存 txt、PDF 类文件将在页面直接显示无法下载。

15.2 APP模糊匹配URL如何设置？

APP 模糊匹配的 URL 设置需要去掉 host 字段，如精确匹配时设置为 `http://www.test.com/test/sys.apk`，那么模糊匹配时 URL 设置成 `/test/sys.apk` 即可，因为模糊匹配时是不会检查 host 字段的，如果设置了 host 字段会导致匹配不上。

15.3 本地文件如果不存在怎么办？

本地文件不存在时，会去源站点下载。

15.4 App缓存文件存储在哪里？

如果有硬盘则存储在硬盘上，如没有则存储在 CF 卡上。

15.5 为什么重启后app缓存计数不正确？

App 缓存命中统计为每小时向文件同步一次，如果出现系统异常或重启，则最近一小时的命中统计数据会丢失。

15.6 APP动态缓存的规格？

APP 动态缓存最多可以写 8 个域名。

15.7 URL链接为什么无法提交？

下载 URL 必须为真实的下载地址，即符合 URL 三要素（资源类型、存放资源的主机域名、资源文件名）。

15.8 CLI下上传的文件能大于剩余缓存空间？

此为软件限制，cli 上传文件，使用的是 tftp 方式。tftp 在上传完成前无法获知上传文件大小。

15.9 磁盘空间大于80%，设备是否还能正常上传app文件？

当磁盘占用率大于 80，无法正常下载。

15.10 页面上动态缓存域名下的已经下载的多个app缓存文件，能否单独删除其中一个app缓存文件？

无法单独删除其中一个 app 缓存文件，只能删除域名同时删除该域名下的所有缓存 app 文件。

15.11 动态缓存的app文件类型？

动态缓存的文件包含（安卓的*.apk）和（苹果的*.ipa）两种类型。

15.12 文件名包含中文时APP动态缓存失败？

使用公网真实的服务器测试不会出现缓存失败现象，测试环境中出现过缓存失败的情况，且只有文件资源名包含中文时才会出现，真实场景是不存在文件名为中文的情况的，目前发现 HFS1.5g 版本搭建的 webserver 服务器当文件名包含中文时其对中文进行编码时使用的中文对照的 16 进制符号不是标准的，会导致设备下载资源后解码出的文件名与实际下载的文件名对应不上，这样即使下载成功了也不能正确显示，测试环境使用的 HFS2.3 版本无问题，推荐使用该版本进行测试，或者直接使用公网环境测试。

15.13 应用缓存功能在PC端连续下载两次文件，缓存计数只命中一次，一次在设备下载，一次在server下载？

应用缓存实现机制：将用户 get 报文截获做 302 重定向到设备本地下载，因为操作过快，导致两次下载的 GET 实际是在同一条流上，因为 302 重定向是针对单条流只会重定向一次，后续的 GET 是直接放通的，所以会出现此现象，是 302 重定向的机制实现。在实际应用场景中，客户端为手机，不存在连续下载多次相同文件的情况，所以在实际应用场景中也就不存在这个问题。

15.14 Smartbits打入混合流量，设备的内存占用较高，此时导入应用缓存，WEB或者Console概率出现错误提示，WEB会处于一直上传的状态？

软件限制，出现概率非常小，不影响使用。

16 会话限制 FAQ

16.1 会话限制基于什么原则来进行限制？

基于会话的源和目的 IP 来进行限制，当会话没有匹配到源 IP 地址，就会继续匹配目的 IP 地址。如果匹配到了源 IP 地址，那么不会继续匹配目的 IP 地址。限制的方式包括并发会话数和每秒新建会话数两种控制方式。

16.2 配置两条会话限制，引用的地址对象分别都包含了某个IP地址，但是会话限制的配置不同，那么该以哪一个为标准？

一条新建的流量能够同时匹配多条会话限制时，将以会话限制配置的从上到下顺序进行匹配，以配置在上面的条目为准。

比如对公司内部各 IP 进行会话数限制，地址对象为 any，总会话数限制为 200，每秒新建限制为 10，对技术支持组的各 IP 进行会话限制，地址对象为 192.168.2.0/24，总会话数限制为 100，每秒新建限制为 10。

配置了两条会话限制，技术支持组的地址对象包含于地址对象 any。

每IP会话限制				
限制策略				
会话统计				
新建				
	地址对象	会话限制	每秒新建限制	操作
1	技术支持组	100	10	编辑 删除
2	any	200	10	编辑 删除

查看限制阻断，匹配到 192.168.2.0/24 的地址的会话限制都采用的是技术支持组的会话限制配置，符合预期效果。

每IP会话限制						
限制策略						
会话统计						
查询 查询条件: 显示全部						
	IP地址	连接数	会话限制	每秒新建	每秒新建限制	限制阻断统计
1	0.0.0.0	1	200	0	10	0
2	192.168.2.1	1	100	0	10	0
3	192.168.2.4	1	100	0	10	0
4	192.168.2.23	2	100	0	10	0
5	192.168.2.129	11	100	0	10	0
6	192.168.2.130	2	100	0	10	0
7	192.168.2.148	1	100	0	10	0
8	192.168.2.185	1	100	0	10	0
9	172.168.100.1	1	200	0	10	0

16.3 会话限制是否可以只限制会话总数，而不限新建会话速度？

可以，会话总数和每秒新建的速度，如果只希望限制一个，可以将另一个的数值设置为 0，表示对该项不进行限制。

16.4 同一个地址对象是否可以配置多个会话限制？

不可以，如果已经配置了某个地址对象的会话限制，那么下一次新建该地址对象的会话限制后，将覆盖之前配置的会话限制。

16.5 在配置会话限制之前，地址对象的会话总数已经超过了该会话限制的会话总数，那么配置该条会话限制后是否会将会话数保持在限制的数目下？

不会，由于会话已经建立，且数量大于当前配置的会话限制中的总数，下一次该地址对象的流量到来后，将不会受到会话限制的影响，除非该会话老化。如果一直有该地址对象的流量通过，那么该会话将无法老化，可以通过手动清除当前的会话，来使得会话限制对该地址对象立即生效。

17 DNS 代理 FAQ

17.1 display dns statistics介绍

query current count: 48977	当前 dns 并发请求数
query total count: 677413	发送的 dns 累计请求次数
cache count: 0	缓存数量
local count: 0	设备 ping 一个域名,成功会+1

17.2 dns规格

dns 并发数可以达到 1W，设备最多允许接收 5W；dns 缓存动态 5 万条，静态和特定域名各 128。

17.3 dns session功能

dns session 主要影响特定域名。
dns session enable 特定域名优先走 session。
dns session diable 特定域名使用特定 DNS 服务器进行动态解析。

17.4 dns缓存达到5w规格后，对新来的dns请求处理

dns 代理缓存达到 5w 以后，新来的 dns 请求继续处理并回应请求端；此时不再对新来的 dns 请求产生的应答进行缓存。

17.5 DNS报文数据段>512后，dns处理

DNS 报文数据段>512，dns 响应报文不能大于 512，对于大于 512 的响应报文，设备进一步回复给客户，但不进行动态缓存。

17.6 DNS接口类型改变后dns无法解析

接口类型改变后必须去手动修改 DNS 链路的配置，否则会造成业务不通。

17.7 DNS A记录显示

A 记录设备最多显示 8 条，如果超过 8，剩下的使用...省略号。

17.8 DNS cache显示

display dns cache 和页面支持显示 4 个具体 ip 地址，后面（）显示总的 ip 地址个数；命令行下 **display dns cache + 域名**可支持最多显示出 8 个具体 IP 地址。

例：

静态域名			
动态缓存			
特定域名解析			
DNS透明代理			
DNS全局配置			
应用 已选择条件:			
域名	TTL	IP	
1 g.cdn.net	70	101.201.172.229;	
2 server24603.beamviewer.com	70	217.146.31.4;	
3 paciao.match.qq.com	13	61.135.157.209;	
4 stockweb.mail.qq.com	422	113.108.11.37;14.17.18.193;	
5 www.airport.us	7	23.42.190.168;	
6 wap.gzhtrip.com	415	220.197.182.60;	
7 sc5.tencent.com	95	183.60.19.151;183.60.19.22;183.60.19.166;183.60.19.167;(16)	
8 translate.googleapis.com	5	203.208.43.102;203.208.43.101;203.208.43.105;203.208.43.103;(11)	

Host Name	Interface	Hit	TTL(s)	IP address
winmo.imap.mail.yahoo.com	ge0	0	148	27.123.207.149 27.123.207.157 27.123.206.201 27.123.207.173 27.123.207.69 27.123.207.165 27.123.206.119 27.123.206.123

17.9 开启DNS透明代理的功能，无法上网

开启 DNS 透明代理的功能，但是没有配置透明代理的策略，仍会命中透明代理的流程，导致用户无法上网，需要配置 dns 透明代理策略。

17.10 域名比较长，页面查询这样的域名是无法查询

如果域名比较长，在页面的 DNS 缓存中无法完全显示（无法显示部分...代替），如果想在页面查询这样的域名是无法查询的。

17.11 设备直接ping域名

本机报文不走 dns 代理流程，只需要在全局 dns 配置一个有效的 DNS 地址(DNS 全局代理可关闭)，在设备上就可以 ping 域名。

17.12 设备dns流程

开启 DNS 透明代理或者 DNS 全局代理其中一个，DNS 流量就会正常的进入 DNS 静态域名，DNS 动态域名流程。

17.13 dns-proxy debug说明

debug 显示出接口为 NULL 时表示匹配的特定域名解析，否则显示出匹配的 DNS 链路出接口，例：
 <2016-12-14 15:07:54> DNSP src ip = 20.1.1.3, dst ip = 200.111.111.1, send target ip = 111.1.1.6, out interface = ge4.4021, domain = www.spirentcom.com, retry = 0
 <2016-12-14 15:07:54> DNSP src ip = 20.1.1.3, dst ip = 200.111.111.1, send target ip = 111.1.1.3, out interface = NULL, domain = 3.33334.www.spirentcom.com.cn, retry = 0

17.14 DNS多链路基于负载

多条链路，配置基于负载，当某个 dns 链路出接口没有路由时，还是会负载 DNS 报文,选到有路由的就发出去,选到没有路由的就发不出去，就会造成部分网络不通。

17.15 多链路DNS基于优先级

多条链路，配置基于优先级，当优先级高的没有到 dns 服务器端路由的时候不会切换到优先级低的 dns 链路发送，会造成网络不通。

17.16 为什么进行包含域名的策略控制会放行一段时间后才可匹配策略？

策略中的地址对象会去 DNS 模块查询匹配，当查询到 DNS 模块中的 IP 和域名的对应关系后，在将原策略中调用的域名对象与 IP 关联来实现策略控制，所以会有短时间的时延。

17.17 客户端A没有配置设备为DNS代理，客户端B配置设备为DNS代理，客户端A发出经过设备的DNS请求，之后客户端B也发出相同域名的DNS请求，设备在对B的请求处理过程是怎样的？

- (1) 在透明代理模式下，当 A 经过设备的 DNS 请求收到响应后，在设备上会产生该域名的动态缓存；如果 B 再向设备发出请求，当设备存有该域名的缓存，并且该缓存的 TTL 时间没有减到 0，那么设备将该缓存直接转发给 B，作为 DNS 响应；如果该动态缓存已经老化，即 TTL 时间减到 0，则向 DNS 代理的服务器发出请求。
- (2) 在全局代理模式下，当 A 经过设备的 DNS 请求收到响应后，在设备上不会产生该域名的动态缓存；如果在 B 向设备发出请求时，当设备存有该域名的缓存，并且该缓存的 TTL 时间没有减到 0，那么设备将该缓存直接转发给 B，作为 DNS 响应；如果该动态缓存已经老化，即 TTL 时间减到 0，则向 DNS 代理的服务器发出请求。

18 攻击防护 FAQ

18.1 扫描攻击防御中的黑名单作用是什么？

在扫描攻击防御中启用加入黑名单功能后，当一个 IP 地址被识别为攻击源后，会被自动加入黑名单，并在设定的时间丢弃所有该 IP 发送的报文。

18.2 配置满规格黑名单后，重复提交IP地址为什么还能提交成功？

新建已存在黑名单，会进行替换，下发成功后会替换之前的名单，并且不会增加黑名单条数，如果已经满规格，进行新的配置，才会给出已超过规格的提示。

19 统计集 FAQ

19.1 统计集统计最近1小时、最近1天、最近1周数据统计的刷新间隔是多少？

统计集中最近 1 小时的刷新间隔是 1 分钟刷新一次，统计最近 1 天的刷新间隔是 10 分钟刷新一次，统计最近 1 周的刷新间隔是 60 分钟刷新一次。

19.2 统计集应用流量统计中所显示的流速计算？

近 1 小时流量趋势图中，将鼠标移动到每分钟上，会显示当时的流速即 1 分钟内流量的平均值；近 1 天流量趋势图中，将鼠标移动到每整 10 分钟时，会显示当时的流速即 10 分钟内流量的平均值；近 1 周流量趋势图中，将鼠标移动到每整小时时，会显示当时的流速即 1 小时内流量的平均值。

19.3 统计集用户统计中用户的类型？

统计集中用户的类型包括匿名用户（IPv4 用户及 IPv6 用户）、静态绑定用户、本地认证用户及第三方认证用户。

19.4 统计集统计用户及应用的规格？

对于不同的系统平台，统计集所显示及统计的用户及应用的规格是不同的，可以通过命令 `display flow-account specification` 查看规格。

19.5 统计集中总流量是如何计算的？

统计集每个应用的总流量为上下数据加下行数据统计出来的总流量，其中总量值后边小数点两位进行四舍五入，所以会造成上行+下行大于或小于总流量现象，误差小于 1%。

19.6 统计集中刷新按钮的作用？

统计集右上角有一个刷新按钮，页面不会自动更新，当用户设置统计集按最近一小时、最近一天、最近一周时，后台分别以 1 分钟、10 分钟、60 分钟进行更新，此时前台页面需要手动点击<更新>按钮进行刷新页面。

19.7 上行流量和下行流量如何区分？

统计集每个应用的总流量为上下数据加下行数据统计出来的总流量，其中总量值后边小数点两位进行四舍五入，所以会造成上行+下行大于或小于总流量现象，误差小于 1%。

19.8 统计集数据是否支持HA？

统计集暂时不支持 HA，即主墙数据不会同步到备墙，当 HA 主备切换后，备墙开始记录数据。

19.9 统计集数据保存重启后是否会丢失？导出再导入是否会丢失？

统计集数据目前不能保存，也不能随配置导出再导入。

19.10 饼图默认显示Top多少？其它应用是什么？

饼图默认显示流量最高的 10 种应用以及其它应用,即 Top10+1,其它应用是指应用总流量小于 0.8% 时，记录到其它应用中。

19.11 统计集中是否会统计出到本地流量？

只统计转发流量，不统计到本地流量。

19.12 当统计集显示页面放大或缩小时，饼图显示变化？

当页面放大或缩小时，饼图的应用注释会与饼图分享，不建议将页面放大或缩小查看。

19.13 统计集是否支持旁路模式？

统计集支持设备旁路模式，能够将 Span 镜像出来的数据进行数据统计。

19.14 统计集中应用统计与用户统计查看区别？

应用统计可以在应用中进行点击，页面跳转到使用该应用的用户页面，用户统计即当前发起流量的 IP 或实名认证用户，点击该用户，可以具体查看该用户所发起的应用流量。

20 地址探测 FAQ

20.1 如何配置track？

进入 WEB 页面内的“对象管理>地址>地址探测”点击新建地址探测。

20.2 为什么ping类型的track状态不稳定？

进入 WEB 页面内的“对象管理>地址>地址探测”查看探测 track 的间隔时间和重试次数是否时间太短。建议探测间隔时间和重试次数使用默认值 10*4。

20.3 为什么tcp类型的探测不成功？

进入 WEB 页面内的“对象管理>地址>地址探测”查看探测 track 状态失败，先确定配置的探测条目 tcp 端口是否打开。

20.4 为什么dns类型探测失败？

- (1) 探测内网的 dns 服务器时，首先确定设备 dns 服务器是否指向了内网 dns 服务器；
- (2) 探测外网的知名 dns 时，首先确定设备是否配置了 dns 服务器，并且配置有到达外网的路由。

20.5 ACG配置HA并且关联track，主墙无法切换？

- (1) ACG 备墙上查看 HA 配置。
- (2) ACG 备墙上查看 HA 所关联 track 状态是否为 Failed。
- (3) ACG 备墙查看引用的 track 对象的探测目标是从哪个接口出去的。
- (4) ACG 备墙在探测目标的接口下配置管理 ip 地址。

20.6 HA联动备墙无法跨网段探测？

- (1) Track 联动 HA 时，因为 HA 备设备只允许源地址为管理地址的报文发送，所以需要将探测报文的源地址指定为接口的管理地址。
- (2) Track 联动 HA 时不支持跨网段的探测，因为跨网段的话，你要把往其它网段的报文发到 HA 管理 IP 的网关上，备设备看来，HA 管理 IP 的网关就是它自己，但是它自己是备状态，报文发不出。

20.7 WEB页面导入csv格式用户和用户组无法同步？

WEB 页面导入 csv 格式用户和用户组后，备墙无法实时同步，需要在主墙同步一次配置后，HA 状态才会一致。

21 策略优化 FAQ

21.1 七元组策略按照什么顺序进行匹配？

当设备中配置了多条七元组策略时，报文会按照一定的顺序与这些规则进行匹配，一旦匹配上某条策略便结束匹配过程。策略的显示顺序与匹配顺序一致，即按照 WEB 界面（或者通过 `display run policy` 命令）显示的顺序，从上到下一次匹配。同时，七元组策略支持通过命令移动策略位置来调整策略的匹配顺序。

21.2 单条七元组审计策略中的应用审计规则、URL审计规则按照什么顺序进行匹配？

单条七元组中可以配置多条应用审计规则和 URL 审计规则。此版本针对应用规则的匹配顺序包括：全匹配、顺序匹配。默认为全匹配，即当报文可以匹配到该七元组策略的多条应用规则（同时包含拒绝、允许两种动作）时，执行拒绝动作。顺序匹配则按照匹配到的第一条应用规则执行。

21.3 添加或修改七元组策略会有什么影响？

添加或修改七元组策略后，所有的流量都会重新进行策略匹配，以使新的策略生效。

22 IMC 联动 FAQ

22.1 如何排查用户无法登录IMC服务器管理页面？

进入 WEB 页面内的“上网行为管理>策略管理>IPv4 策略”查看 ACG 设备中是否有策略将流量拒绝或进入“网络配置>路由>路由表”查看是否存在 IMC 服务器地址路由条目。

22.2 为什么认证时无法接收认证推送页面？

进入 WEB 页面“用户管理>认证服务器>Portal Server”中查看“认证 URL”是否正确。配置 URL 时，根据“例如”信息，将 Server ip 地址更改为服务器的 IP 地址。

22.3 使用NAT用户通过认证后访问外网页面依然弹出认证页面，导致循环认证？

在 NAT 环境中，用户访问服务器时 MAC 地址会发生更改。导致服务器接收的 MAC 地址与接入用户的 MAC 不符，产生循环认证的问题。命令行中使用 `user-portal-server mac-sensitive enable` 可解决。

22.4 为什么认证时，可以接收推送认证页面，用户名密码输入完毕后无法认证成功？

- (1) 首先在接收的认证页面中输入正确的用户名密码“上线”后，错误信息“向设备发送请求失败。可以检查设备中 RADIUS 服务器端口号是否与 IMC 服务器端端口号相同；
- (2) 查看输入的用户名、密码与 IMC 服务器中配置的接入用户信息不一致。可查看 IMC 服务器中接入的用户名、密码是否与输入的相符；
- (3) 查看 IMC 服务器内的“用户>接入策略管理>Portal 服务管理>IP 地址组配置”查看认证用户的 IP 地址范围是否在 IP 地址组范围内。

22.5 为什么用户认证时点击一次上线，显示设备拒绝请求，点击多次后可认证成功？

ACG 内将 RADIUS 组调用在 Portal Server 中，该组内有多个 RADIUS 服务器存在，配置与 IMC 服务器相同的 RADIUS 服务器不是该 RADIUS 组中第一个 RADIUS 服务器。所以需要进行多次 RADIUS 服务器匹配，当匹配到与 IMC 服务器相同 RADIUS 服务器时即可认证成功。

22.6 登录超时后重新认证，在认证窗口填写用户名密码后点击“上线”提示“用户已在线”？

用户的 PC 上原认证页面未关闭，将原认证页面关闭或在认证页面填写已认证用户名、密码、服务后，点击下线后，可正常重新认证认证。

22.7 为什么认证模板设置IE10浏览器没有调色板按钮, 只能通过数字设置认证按钮颜色？

在浏览器调用调色板时需要浏览器支持 color 类型。只有支持 color 类型的浏览器才可看到颜色按钮，如不支持的浏览器则会出现此问题现象。

这个问题并非 ACG 选用调色板插件问题，主要在于浏览器的支持 color 情况。目前已知的浏览器限制有 IE 和 Safari 两款浏览器，因与浏览器相关，ACG 不可控，故将此问题定位为软件限制，在发布说明书中体现。

22.8 用户在线时间超出所配置的超时时间，有时可下线、有时不可下线？

- (1) 配置超时时间分为两项，一项是 IMC 服务器上配置的用户在线时长，另一项是 ACG1000 的 Portal Server 页面配置的超时时间，当 IMC 服务器和 ACG1000 同时配置超时时间，这样会在两者内选择一个最小值最为最终的超时时间。当用户在线时长触及了最小超时时间，用户立即下线；
- (2) 当 IMC 服务器未配置用户在线时长，仅在 ACG1000 的 Portal Server 内配置超时时间，在这样的情况下，用户的超时会以在超时时间范围内是否有流量来衡量用户是否超时下线。当在超时时间范围无流量产生，则该用户被下线。有流量产生，则按流量停止时间开始计算，闲置时间超出配置的超时时间，用户被强制下线。

23 第三方用户存储认证

23.1 如何排查用户无法登录Radius（IMC）服务器管理页面？

- (1) 首先查看 ipv4 策略是否将此数据包拒绝；
- (2) 查看 ACG 设备路由是否正确；
- (3) 查看用户策略的目的 IP 是否将服务器的 IP 地址排除在外。

23.2 为什么认证时无法重定向到认证页面？

- (1) 首先查看 ipv4 策略是否将此数据包拒绝；
- (2) 查看 ACG 设备路由是否正确；
- (3) 查看用户策略是否正确，PC 上网时是否匹配到此用户策略。

23.3 输入用户名及密码后，认证失败，提示“用户名或密码错误”，如何定位认证失败原因，并及时修改？

根据 `debug aaa event` 或系统日志信息查看，认证失败原因：

- (1) 服务器无响应：查看路由及 IPV4 策略是否正确；服务器端口是否匹配；
- (2) 服务器密码错误（指 Radius）；
- (3) 用户名或密码错误：查看所输入的用户名是否与第三方服务器上的用户名一致；确定密码是否正确，与服务器上对应用户名的密码一致。特别需要指出的是对于 Radius 第三方用户存储认证，所使用的服务器为 IMC 服务器中的 Radius 部分，所以输入的用户名还要包括服务类型标识部分，账号与服务类型之间用@连接，如 `htest@kkk`，其中 `htest` 表示账号名称，`kkk` 为服务类型标识，这两者用@连接后整体作为认证用户的用户名。

23.4 在页面认证服务器>本地Web认证页面，在用户登录唯一性检查项，配置单一账号登录，并禁止禁止同名用户再次登录后，为什么用户第三方 Radius认证对于同一账号仍能多次登录？

对于这种第三方的用户，是否允许用户重复登录，应该由认证服务器去做限制，本地认证的配置只能对本地用户做限制；用户第三方 Radius 认证使用的服务器为 IMC 服务器，服务器中对于每个账号都有上线人数限制，但对于接入设备类型为 UNIS(General)设备，此上线人数限制暂时不起作用。

24 断点续传 FAQ

24.1 什么情况下属于断点续传？

属于断点续传的有服务器不可达/服务器 `down/vtysh` 超时退出（这种情况下，属于断点下载范围。当设备版本下载过程中断掉后，再次开始后从上一次的进度处开始下载）。下载过程中，用户主动断掉（`ctrl+c`，这种情况不属于断点下载，需要重头开始下载）。

25 会话统计 FAQ

25.1 会话统计排名为什么只有前50个？

会话统计的排名是按照会话连接数的多少进行的排名，默认只显示前 50 个会话的排名。

25.2 会话监控页面有的会话存在时间为0秒？

原因是当一条流老化后，又重新产生了一条这样的流，此时存在时间就为 0 秒。这种情况大多出现在清流过后，立即在 web 监控页面查看会话监控，容易出现此情况。

26 抓包工具 FAQ

26.1 抓包工具开始抓包后，什么情况下停止抓包？

当用户抓包达到 20M 或者 300s 时自动停止抓包或者也可以手动停止抓包。

26.2 抓包工具高级选项里的抓取新建会话是什么意思？

抓取新建会话：新的五元组信息产生的新的流。当高级选项抓取新建会话为 2 时，指的是一条新建流的前两个包。

27 日志分析与管理平台部署方式 FAQ

27.1 ACG1000日志分析与管理平台运行环境要求有哪些？

ACG1000 日志分析与管理平台推荐安装在 64 位的操作系统上，包括 windows 7/windows XP/windows server 2003/windows server 2000。

系统运行环境最低配置为：PC 服务器/Pentium IV CPU/4G 内存/100G 以上存储空间，最好是磁盘阵列。系统运行环境建议配置为：PC 服务器/Pentium IV CPU/16G 内存/500G 以上存储空间，最好是磁盘阵列。

27.2 ACG1000日志分析与管理平台有哪些端口被占用？

端口占用说明：web 服务(80 端口)，日志服务器(514 端口)，数据库(60005 端口)，内部服务(60006 端口)，ftp 服务器（21 端口），请确保以上端口不被别的程序占用。

27.3 ACG1000日志分析与管理平台管理员客户端有哪些要求？

硬件环境 PC 机或笔记本/Pentium II CPU / 512M 内存，软件环境 IE9.0 版本、Mozilla21.0 版本浏览器，最佳显示分辨率为 1366×768。

27.4 安装完成后打不开ACG1000日志分析与管理平台提示端口被占用怎么办？

由于我们 ACG1000 日志分析与管理平台是安装在服务器上，有可能和其他厂家类似软件产生冲突，建议保持服务器纯净尽量少安装其他软件，如果遇到错误（以 80 端口占用为例）请用以下步骤查找原因。

- (1) 在 CMD 模式下执行命令 **netstat -aon | findstr 80** 占用 80 端口的进程，然后执行 **msinfo32** 命令查看正在运行的进程的 ID 的安装路径卸载该程序或者停止它，如果还遇到问题请卸载重启之后安装。

- (2) 由于 win2003 服务器由于自带服务 “World Wide Web Publishing Service” 占用 80 端口所以请先停止该服务在安装。控制面板>管理工具>服务，打开服务找到 “World Wide Web Publishing Service” 右键选择停止即可。

27.5 如何设置映射端口使ACG1000日志分析与管理平台可以接收到ACG设备的信息？

模拟场景：ACG1000 日志分析与管理平台在北京总公司，连接某一台防火墙，另外 ACG 设备在其他地方，这样就需要在 ACG1000 日志分析与管理平台和防火墙进行端口映射，设备需要访问 ACG1000 日志分析与管理平台的 514，21 端口。ACG1000 日志分析与管理平台需要访问设备的 8888 端口，访问 ACG1000 日志分析与管理平台的服务器需要 80 端口。

27.6 ACG1000添加到管理平台后，点击ACG1000页面的“数据中心”无法打开？

ACG1000 页面的“数据中心”连接固定的 80 端口，且不支持修改，如果管理平台将端口修改为非 80 端口就会导致无法连接，此时建议在浏览器中手动输入管理平台的访问地址和正确的端口号即可正常连接访问。

28 日志分析与管理平台程序管理 FAQ

28.1 ACG1000日志分析与管理平台默认登录用户名和密码是什么？

系统默认的管理员用户为 super，密码为 super.123。用户可以使用这个管理员账号从任何可访问设备的地址登录设备，并且使用设备的所有功能。

系统有三权分立默认账户分别为：

- (1) 审计管理员：用户名为 admin_audit，密码为 audit.123。
- (2) 配置管理员：用户名为 admin_config，密码为 config.123。
- (3) 用户管理员：用户名为 admin_user，密码为 user.123。

28.2 ACG1000日志分析与管理平台的SYSLOG端口是多少？

系统默认的 syslog 接收端口为 514。

28.3 ACG1000日志分析与管理平台使用什么浏览器比较好？

通过运行浏览器对 ACG1000 日志分析与管理平台软件进行配置和管理。ACG1000 日志分析与管理平台安装之后默认开启了 web 服务。

请用户使用 IE9.0、Mozilla21.0 版本浏览器对 ACG1000 日志分析与管理平台进行 web 管理。

28.4 打开ACG1000日志分析与管理平台登录界面看不到验证码怎么办？

将服务器 ACG1000 日志分析与管理平台软件的服务重新启动。

28.5 打开ACG1000日志分析与管理平台接收不到日志怎么处理？

- (1) 查看 ACG1000 日志分析与管理平台是否可以管理到该设备。
- (2) 查看设备端的日志设置的日志服务器 IP 地址是否填写正确，日志过滤里是否记录并且发送日志。
- (3) 查看设备端的安全策略是否填写记录上网行为。
- (4) 查看 ACG1000 日志分析与管理平台服务器的服务是否都已经开启了。

28.6 用户登录后可以在哪里修改密码？

系统管理>管理员>选择用户>点击编辑密码，就可以进入修改该用户密码界面。

28.7 用户打不开ACG1000日志分析与管理平台怎么办？

查看服务器上 ACG1000 日志分析与管理平台的服务是否都已经正确开启，浏览器选择是否正确。

29 日志分析与管理平台设备管理 FAQ

29.1 如何添加设备？

设备管理>设备管理>添加设备，填写正确的设备 IP 地址、用户名、密码，点击<确定>按钮就完成添加一台设备。

29.2 如何查看添加到设备组的设备？

在设备管理界面的左侧，有设备组，选择设备所在的设备组，点击进入查看，查看设备是否正确分配到指定设备组。

29.3 正确添加好设备后为什么设备状态显示未在线设备？

- (1) 在确定设备 IP 地址正确，用户名密码填写正确的情况下，如果设备显示未上线状态，查看设备电源是否断电，设备线路连接是否无误，路由转发是否正确。
- (2) 设备端没有问题但就是依然无法连接到设备，查看是否当前经过设备的流量过大。导致设备超负荷而无法连接。
- (3) 某些设备默认情况下的端口 `center-monitor` 是关闭的，需要开启，进入设备命令行，输入 **display running-config** 查看连接端口是否开启 **allow access center-monitor**。如果没有开启的话，进入设备命令行，进入管理连接端口，执行命令 **allow access center-monitor**。

29.4 最多可以管理多少台设备？

如果不进行授权，只允许最多添加 9 台低端设备（ACG1000-C 和 ACG1000-S），不允许添加高端设备。

授权包括：高端授权和集中授权，单独完成高端授权允许添加低端设备和高端设备，最大数量为 9 台。

单独完成集中授权允许添加低端设备 500 台，不允许添加高端设备。如果同时完成高端授权和集中授权，那么允许添加低端设备和高端设备共 500 台。

29.5 如何在ACG1000日志分析与管理平台直接进入设备管理界面？

在 ACG1000 日志分析与管理平台的设备管理里，根据选择进入哪台设备点击后边的 WEB 界面，就可以进入这台设备的管理界面。

29.6 如何能够更方便的管理设备？

可以进行分组存放设备，在设备管理界面，点击添加，添加设备组，新建一个设备组后，可以将设备按照一定要求存放在你想放的设备组里，这样就很大程度上的方便了管理设备。

29.7 导出设备管理是全部导出，还是只导出某一组的设备？

全部设备信息都导出。

29.8 如果设备突然掉线了怎么办？

设备突然掉线，修复故障后，点击这台设备后面的<操作>按钮，会尝试重新连接，如果 IP 地址，用户名，密码，并且设备正常运行，那么就会重新连接上。

29.9 想将设备进行重启，怎么操作？

点击设备管理下面的设备升级，选择需要重启的设备，点击左上方的<重启>按钮即可。

29.10 当设备太多了，找不到想管理的设备怎么办？

在设备管理界面有搜索功能，并且功能支持模糊搜索，只要知道设备的名称、设备 IP、设备 SN 其中的一项就可以在搜索里进行搜索，并且可以快速找到要管理的设备。

29.11 设备添加信息错误了，如何修改？名称可以修改吗？

对已经添加的设备进行修改，先选择设备，然后点击<修改>按钮，就可以对设备进行从新的定义，但是设备名称是不可以修改的。

29.12 如果删除此设备后，之前此设备的日志还存在吗？

如果删除一台设备后，这台设备之前的日志也会被清空。

29.13 如何通过EXCEL导入设备

首先在 ACG1000 日志分析与管理平台设备管理界面下载一份模版,根据模版正确的填写设备名称、设备 IP、用户名、密码、设备型号后,保存,在设备管理点击导入,信息填写正确可以完成导入,如果信息填写错误导入后则会提示导入失败,并且有失败原因。

29.14 如何使用自动探测和自动下发文件功能?

在设备管理页面的文件下发任务中包含自动探测配置,在自动探测配置里,用户可以选择是否开启自动探测任务,并且设置自动探测任务时间,还有选择是否开启自动下发所有任务,并且设备自动下发所有任务的时间。设置好,自动探测和自动下发后,在文件管理中,新建一个正确的 URL 地址和名称后,在规定的时间内就可以自动探测和自动下发文件到所有设备中。

29.15 是否支持所有的URL格式的自动探测?

日志分析与管理平台只支持 http 协议的 URL 自动探测。

29.16 日志分析与管理平台对服务器内存是否有要求?

服务器内存可用内存不足 4G 的,但使用效果可能无法达到预期效果。

30 日志分析与管理平台监控统计 FAQ

30.1 监控统计都包括哪些信息?

监控统计包括 4 大部分:系统状态、设备流量监控、用户流量监控、应用流量监控。

30.2 在监控统计中可以调节的参数有哪些?

可以调节的有:选择设备、时间范围、统计依据、显示前多少项、选择用户、过滤条件。

30.3 系统状态包括哪些信息?

- (1) 管理状态:时间、软件版本、数据库大小、数据库版本、磁盘空间大小、设备数量情况、授权信息、可以管理最大设备数。
- (2) 最新报表汇总:最近生成的报表任务信息。
- (3) 最近一天日志数量统计:设备操作日志、系统事件日志、流量日志、NAT 日志、网站访问日志、聊天日志、恶意网站访问日志。
- (4) 最近一天设备流量统计:用柱状图表示设备最近一天经过有多少流量。

30.4 设备流量监控包括哪些信息？

点击设备流量监控可以查看所有设备在某一段时间的流量统计，并且在下方会有设备流量排名信息，点击设备的柱状图会跳转到流量趋势界面，可以看到某一段时间内的流量情况，其时间间隔根据选择查看的日期而不同，在流量趋势界面的下方会有用户和应用的排名。回到流量排名界面，在下方设备流量排名点击某一台设备的用户排名会跳转到用户流量排名，并且是根据当前设备来判断的，回到流量排名界面，在下方设备流量排名点击某一台设备的应用排名会跳转到用户应用排名，可以看到哪些应用用了多少流量，并且是根据当前设备来判断的。

30.5 用户排名流量监控包括哪些信息？

选择好要查看的设备后，会看到这台设备的所有用户的流量排名，点击下方的用户应用排名，会看到这个用户都有哪些应用产生了多少流量从大到小排列。

30.6 应用流量监控包括哪些信息？

选择好要查看的设备后，会看到这台设备的应用流量情况柱状图，可以看到都有哪些应用产生了多少流量，点击下方的应用用户排名可以看到，同一个应用哪个用户的流量多少。

30.7 不同范围的波形图的时间间隔是多少？

- 时间范围：最近一天，波形图时间间隔：10 分钟。
- 时间范围：最近一周，波形图时间间隔：1 小时。
- 时间范围：最近一月，波形图时间间隔：4 小时。
- 时间范围：最近一年，波形图时间间隔：1 天。
- 时间范围：自定义时间，波形图时间间隔：参考上面 4 个范围，给出间隔时间。

30.8 某一台客户端查询不到设备流量，但是另外一台管理相同设备的 ACG1000 日志分析与管理平台却可以查询的到，这是什么原因？

可能的因素如下：

- (1) 服务器 ACG1000 日志分析与管理平台的服务没有开启。
- (2) 在设备端的日志设定中的日志服务器没有选择服务器 IP 地址。
- (3) 这台客户端的流量表损坏。
- (4) 确定连接线路没有故障。

31 日志分析与管理平台策略管理 FAQ

31.1 地址对象的基本操作都有哪些？

可以添加、修改、删除、克隆地址对象，按照正确的要求添加地址对象后，在地址对象界面会出现新添加的这条地址对象，用户可以对这条地址对象进行：修改、删除、克隆等操作。在成功添加地址对象后，在其他的项目中可以引用正确添加的地址对象，比如：地址组对象、集中策略中的源/目的地址，都可以引用正确添加的地址对象。其重要作用就是将部分 IP 地址归结到一起，方便以后的使用。

31.2 服务对象的基本操作都有哪些？

在服务对象中包括：自定义服务对象，可以按照要求添加新的服务，服务组对象，将部分服务综合起来利于大家的发展，预定义服务器，系统默认的服务，不允许修改，但是允许引用。

对于自定义服务对象，服务组对象可以进行添加、修改、删除、克隆操作，并且成功的添加服务对象后，可以被策略管理所引用，用来管理服务。

31.3 时间对象的基本操作都有哪些？

时间对象可以添加的计划有：单次计划，每日计划，每周计划。

- 单次计划：只执行一次，可以对单次计划进行添加，删除，修改，克隆操作。
- 每日计划：每天固定的时间执行，可也是多个时间段，可以被每周计划引用，可以对每日计划进行添加，删除，修改，克隆操作。
- 每周计划：可以安排一个星期的计划，每周计划不允许为空，但是允许其中的某几天计划为空，并且可以引用每日计划，但是不能引用单次计划。可以对每周计划进行添加，删除，修改，克隆操作。

31.4 应用对象的基本操作都有哪些？

对于应用对象，不可以进行添加，修改，删除等操作，但是可以通过系统文件来升级应用对象。应用组对象，引用多个应用对象，组成新的应用组对象，可以进行添加，删除，修改操作。

应用对象和应用组对象可以被策略管理中的应用选择所引用，但是新建的应用组对象不能被策略管理的应用过滤引用，应用过滤只引用系统的应用对象。

31.5 URL对象的基本操作都有哪些？

- 预定义 URL 分类，不可以进行添加，修改，删除等操作，只能通过系统文件来升级 URL 分类。
- 自定义 URL，可以进行添加、修改、删除、克隆操作。一个自定义 URL 里可以包含多个 URL。
- 在策略管理的 URL 过滤中，可以应用系统的 URL 分类，也可以引用自定义的 URL。

31.6 关键字对象的基本操作都有哪些？

可以添加新的关键字，并且成功添加一条关键字以后，可以对其进行修改，删除，克隆操作。在策略管理中的应用过滤里，有关键字匹配，在那里可以应用成功添加的关键字。

31.7 集中策略如何下发？

在集中策略里点击<添加>按钮，按照需求进行配置，正确配置以后，点击<确定>按钮，此时在策略管理界面会出现新添加的集中策略，选择这条集中策略，点击上方红色<下发>按钮，此时会弹出选择设备对话框，选择要下发到哪一台设备，点击确定，如果没有问题则提示，下发成功，如果有问题则提示下发失败。

31.8 如何查看下发失败原因？

如果一条策略下发失败以后，这条策略的下发结果为下发失败，点击左侧的设备名称查看具体失败原因。

31.9 策略成功下发在设备端哪里可以找到？

如果一条策略成功下发以后，打开设备的上网行为管理-策略配置-IPv4 策略，就可以看到刚刚下发的策略，并且 ACG1000 日志分析与管理平台下发的策略的优先级最高。

31.10 可以同时多个策略下发吗？

不允许同时下发多条策略，但是允许同一条策略同时下发到多台设备。

31.11 可以对策略进行什么操作？

有修改，删除，下发操作，都可以正确的执行命令。

32 日志分析与管理平台日志查询 FAQ

32.1 日志查询有哪些作用？

用户可以通过不同行为的查询，查询到设备上的用户在某些时间段内的具体操作，可以有效的统计和管理。

例如想要查看用户今天都访问了哪些网站就可以选择日志查询-上网行为日志-网站访问，在设置界面选择要查看的设备，选择要看的用户 IP 地址，时间选择最近一天，点击<确定>按钮，就会出现这个用户最近一天都访问了哪些网站。

32.2 日志查询是通过什么来查询数据的？

日志查询是通过查询数据库中的表来返回查询结果的。

例如数据库中表:t_log_nat_201408 存储的就是 2014 年 8 月份的 NAT 日志,表 t_log_other_201409 存储的就是 2014 年 9 月份的其他日志审计的日志等等,日志查询就是通过查询不同的项目,找到对应的表来返回表中的结果。

32.3 如何进行日志查询?

选择要查询的日志种类,选择要查询哪台设备,选择时间段,之后点击<确定>按钮就会出现这台设备在这段时间内的操作。

例如:要查询设备:192.168.2.55 在最近 1 天内的网站访问日志,操作过程:

- (1) 点击“日志查询>上网行为日志>网站访问”
- (2) 选择设备地方不选择全部设备,选择 192.168.2.55 这台设备
- (3) 创建时间选择最近一天 6、点击<确定>按钮。

这样就会出现 2.55 这台设备最近一天的网站访问日志。

32.4 正确的查询步骤,为什么没有日志?

没有查询的日志的原因可能如下:

- 客户端日志过滤选项没有配置发送到 syslog 服务器。
- 在设备端的日志设定中的日志服务器没有选择服务器 IP 地址。
- 设备端的相应功能是否设置为记录日志。
- 这台客户端的流量表损坏。
- 确定连接线路没有故障。
- 利用抓包工具查看是否有日志信息发过来,没有的话则是设备端没有发送日志,去查看设备端是否产生了日志,如果发送过来了,则是日志没有入库,可以稍等 1 分钟。

32.5 日志查询都可以设置哪些过滤条件?何时使用?

过滤条件有:选择设备,筛选用户,过滤源地址和目的地址,URL 分类过滤,域名过滤,URL 过滤,动作过滤,级别过滤,筛选时间段。

如果在管理很多台设备,需要查询一台设备里的某一个用户,就可以用到日志过滤查询功能。

32.6 日志查询的效率受哪些因素的影响?

日志数量的多少、用户的多少、是否涉及多个月份、过滤条件、此时是否有数据存储。

33 日志分析与管理平台统计报表 FAQ

33.1 统计报表有哪些作用？

通过新建报表任务或者预定义报表任务，可以查询到某台设备的每周，每月，某个时间段的设备流量，上网行为，网络总体，关键字用户，应用审计的具体信息，将以柱状图，波形图，饼图等形式展示出来。可以方便用户对设备的管理和统计。

33.2 报表文件，报表任务，预定义报表任务都是用来做什么的？

报表文件是通过报表任务或者预定义报表任务执行得到的关于某台设备在某段时间行为的统计数据。

报表任务是用户自己定义的任务形式，其中可以选择表报任务的行为有：设备流量、上网行为、网络总体、关键字用户、应用审计。在统计内容中具体选择哪个报表模块，设置统计条件，设置生成时间，选择生成格式即可。

预定义报表任务是程序自带的报表任务，总共包括：每周设备应用流量报表，每周设备用户流量排名，每周设备流量排名，月度设备应用流量排名，月度设备用户流量排名，月度设备流量排名。预定义报表任务只能修改名称和设备，其他的选项为固定的。

33.3 设备状况为未选设备，无法生成报表是什么情况？

这样的提示说明此时没有连接到你的设备，请点击<编辑按钮，选择要生成报表的设备即可。

33.4 产生的报表文件都有什么格式的？

报表文件的格式分为：HTML 或者 PDF。在编辑表报任务的生成格式可以选择 HTML 格式和 PDF 格式。

33.5 报表任务可以选择几台设备？

选择设备时只允许选择一台。

33.6 点击立即执行，为什么没有报表文件？

等待一会，生成报表文件需要一定的时间，如果等待一会也没有报表文件出现，查看报表任务执行是否正确。

34 日志分析与管理平台系统管理 FAQ

34.1 在哪里修改管理员密码？

在系统管理-管理员可以选择 **super** 超级管理员进行修改密码。

34.2 能否自己为管理员分配权限？

使用超级管理员可以为其他管理员分配权限，在系统管理-管理员-角色管理中可以为管理员分配权限。

34.3 如果其他新建管理员忘记密码如何找回？

可以通过使用 **super** 账号，对丢失密码的管理员进行密码重置，从而找回密码。

34.4 如何备份数据库？

在系统管理>数据库备份还原中输入正确的备份路径，就可以将当前的数据库备份到路径文件下。

34.5 如何还原数据库？

在系统管理>数据库备份还原中输入正确的还原路径和文件名称，就可以将备份的数据库还原到现在数据库上。

34.6 如何进行日志备份？

在系统管理>日志备份还原中选择要备份的日志类型，也可以多选和全选，选择要备份日志的日期，填写正确的备份路径，就可以将选择的日志备份到填写的路径文件下。

34.7 如何进行日志还原？

在系统管理>日志备份还原>日志还原，填写正确的还原文件的路径和文件名称，点击<确定>按钮，就可以将备份的日志还原到 **ACG1000** 日志分析与管理平台上。

34.8 数据库配置自动备份后存放在哪里？

自动备份的数据库存放在配置自动备份时填写的路径内，可以通过查询备份结果确定。

34.9 数据库备份结果页面显示哪些信息？

数据库备份结果页面会显示自动备份数据库信息和立即备份当月数据库信息，不会显示立即备份全部的数据库信息。

34.10 数据库备份还原注意事项有哪些？

- 数据库备份和还原时，服务会关闭，所以在执行数据库备份还原时需要注意数据会不入库。
- 在还原的时候一定要按照备份时间顺序还原，否则有可能导致数据异常。

34.11 设备批量重启增加哪些功能？

在重启设备时可以选择是否保存配置，如果仅仅重启设备，不会保存设备的配置信息，如果选择设备重启并且保存配置会先保存设备的配置信息，保存成功后，重启设备。

35 服务质量管理 FAQ

35.1 服务质量管理条目“最后一次成功率”和“最后一次延时”在建立前的时间也有数据显示？

对于服务质量管理条目建立之前的“最后一次成功率”和“最后一次延时”数据进行补零显示；

35.2 为什么tcp类型的服务质量管理条目探测结果为零？

进入 WEB 页面内的“网络优化>服务质量管理”查看探测结果，先确定配置的探测条目 tcp 端口是否打开。

35.3 为什么dns类型的服务质量管理条目探测数据一直为零？

- (1) 探测内网的 dns 服务器时，首先确定设备 dns 服务器是否指向了内网 dns 服务器；
- (2) 探测外网的知名 dns 时，首先确定设备是否配置了 dns 服务器，并且配置有到达外网的路由。

35.4 为什么debug service-quality不显示dns类型的服务质量管理条目发送的探测报文？

当设备上未配置 DNS 服务器时会出现以上情况：

- (1) 探测内网的 dns 服务器时，首先确定设备 dns 服务器是否指向了内网 dns 服务器；
- (2) 探测外网的知名 dns 时，首先确定设备是否配置了 dns 服务器，并且配置有到达外网的路由。

36 基于用户 MAC 的转发策略 FAQ

36.1 在ACG上配置有用户认证策略，并新建用户将PC的MAC地址绑定，为什么PC仍无法上网并重定向到认证页面？

PC 能够重定向到认证页面，说明设备的路由及 IPV4 策略是没有问题的。

- (1) 首先查看绑定的 MAC 地址是否与 PC 的 MAC 地址一致；
- (2) 再查看下组网方式，若是 ACG 通过三层交换机与内网 PC 相连，目前 ACG 没有跨三层 MAC 地址学习功能，则无法直接获取到内网 PC 的 MAC 地址，这样即使绑定了 MAC 地址，仍然需要通过认证才能上网。

37 链路负载均衡 FAQ

37.1 负载均衡使用场景？

- (1) 多出口场景下使用。
- (2) 接口最少 2 个最多 4 个。
- (3) 目前不支持 ISP 就近探测。
- (4) 如果在出口使用的话路由需要配置为默认等价路由。且在同一负载均衡组下。
- (5) 如果一个路由的多下一跳出口分属不同的负载均衡组，对于这种存在冲突的情况，按照之前的路由选路方式进行，不再进行负载均衡。
- (6) 只有物理口能加入负载均衡组。
- (7) 加入到负载均衡组中的接口不能再加入到桥口或聚合口和 HA 心跳口。

37.2 负载均衡支持的负载方式？

目前支持带宽比负载和优先级负载两种方式。

37.3 带宽比的负载方式使用的算法？

根据每条链路的带宽，通过分配新建链接，采用轮询负载均衡接口的方式选择出口，达到负载均衡的目的。

37.4 带宽比负载使用条件？

- (1) 必须有两个出口。
- (2) 只有加入到负载均衡的接口，且路由可达的接口才对流量做负载均衡。
- (3) 采用带宽比负载均衡时，接口组里的所有接口都需要配置带宽，否则该接口组不生效，阈值可不配置。
- (4) 不配置阈值的情况下，按照带宽比例进行负载。配置阈值的情况下，根据接口带宽和阈值的值进行转发。
- (5) 如果没有配置过载保护接口的话，当链路阈值到达后，该链路不再承载新连接的流量，转由其他链路进行负载。当所有链路都达到阈值后，则会对新连接丢包。
- (6) 如果有多个过载保护口，只选择当前负载最小的接口。

37.5 优先级定义

基于优先级的是 谁的优先级高先走谁 接口达到阈值后在找第二优先级的接口走，相同优先级,接口流量满了后才从其它接口转发。

37.6 负载方式为优先级的使用条件？

- (1) 必须有两个出口。
- (2) 只有加入到负载均衡的接口，且路由可达的接口才对流量做负载均衡。
- (3) 接口必须配置优先级。默认优先级为 4，数字越小，优先级越高。带宽阈值可不配置。
- (4) 负载方式为优先级并且配置有接口带宽和阈值，当优先级高的链路达到阈值后，走优先级低的链路。

37.7 会话保持与带宽比结合使用

- (1) 负载方式为带宽比的情况下，会话保持优于带宽比。
- (2) 会话保持保证同一源 IP 出接口一样。如 FTP 控制流和数据流走同一链路，同一用户的请求能持续在同一个链路进行负载，避免网银等业务不可用。

37.8 会话保持与优先级

- (1) 负载方式为优先级，同时开启了会话保持，先走优先级。
- (2) 会话保持对优先级无效，因为优先级强调的本来就是优先走哪个接口，这俩互斥。

37.9 过载保护使用说明？

- (1) 负载均衡组指定过载保护接口,该接口在负载均衡组中。当负载均衡的各个出口都达到阈值后，再有新建会话则从指定的过载保护口出，并且该口不受阈值限制。
- (2) 如果有多个过载保护口，只选择当前负载最小的接口。

37.10 健康检查

支持在负载均衡接口上配置健康检查，引用已有的 track 机制。当 track 状态发生变化时，对应接口的路由状态发生变化。基于 track，已实现 ICMP、TCP（HTTP、FTP、DNS 等）。对于需要多种检测方式的，引用 track 组。

38 三权分立 FAQ

38.1 三权模式下各管理员的职责？

账号管理员：创建/删除/编辑系统管理员账号以及查看自己的操作日志。

权限分配管理员：为系统管理员分配权限以及查看自己的操作日志。

审核员：可以查看所有管理员的操作日志。

系统管理员：对自己已有权限的模块行进操作。

38.1.1 三权模式可以切换到普通模式吗？

设备由普通模式切换到三权模式后，不能再切换到普通模式。

38.2 三个默认管理员账号是否可编辑？

账号管理员、权限分配管理员、审核员这三个默认管理员的名称和密码都可以修改。

38.3 普通模式切换到三权模式后，原来的系统管理员、审计员账号还可以登录吗？

设备由普通模式切换到三权模式后，原来的系统管理员和审计员都成为系统管理员，但权限为空。

39 广告推送 FAQ

39.1 广告对象规格

广告对象配置支持 16 条。

39.2 广告策略规格

广告策略配置支持 16 条。

39.3 广告策略引用广告对象规格

一条广告策略可引用 1-3 个广告服务对象。

39.4 广告对象里图片规格及限制

本地广告服务对象最多支持 4 张图片，图片格式目前支持 jpg、png，不支持动态图片上传 gif,不支持 bmp 格式图片。

39.5 广告策略引用广告对象限制

策略中引用的广告对象必须种类相同，不可第三方及本地同时引用。且被引用的广告对象不可修改类型。

39.6 广告对象命令行限制

命令行不支持新建广告对象。只能修改一些参数，图片不支持修改，命令行主要做配置恢复。

命令行不支持图片导入，不支持图片 ha。

39.7 广告策略引用对象位置

一条策略里三组图片，如果图片位置一样的话，pc 访问页面广告覆盖显示。

39.8 广告对象和广告策略里设备IP的使用

广告对象里的设备 ip 不通的情况下广告图片无法加载;策略里地址对象不通导致 web 页面打不开。

39.9 域名白名单匹配规则

域名白名单模糊匹配（使用简单的字符串匹配）。配 xw.qq.com 访问 www.xw.qq.com 这才是包含关系。

39.10 手机端广告图片展示限制

手机广告对象弹出只有置中与广告对象上下左右不一致。广告对象位置信息只针对 PC 端生效，移动端全屏显示。支持配置多张图片，以轮播的形式展示，最多支持 4 张，且每张图片支持广告 URL 及描述配置。

39.11 广告策略跨网段使用限制

广告推送如果跨网段推送广告。需要下联用户的入接口开启 http 服务（推送模板需要基于设备的一些 js 库，需走设备入接口 http 服务）。

39.12 手机端浏览器使用限制

手机端 UC 浏览器需要关闭广告过滤推送的广告才能显示。

39.13 微博类网站广告使用限制

腾讯微博和新浪微博内置了域名白名单不会弹送广告。

39.14 一些网站不弹广告

某些网站安全检查走的是云加速，存在 302 跳转导致无法打开。开启云加速功能后无法抓到第一个 GET 包，目前手机 qq 浏览器需关闭“云加速”后才能够弹出广告。

39.15 邮箱类不弹广告

163 和 126 邮箱页面和广告模板存在兼容问题，不推送广告。

39.16 开启广告推送后，一些网页打不开

由于某些网站类型限制，导致插入广告后会存在网页打不开现象。网页刷新三次后可以打开（为了提高推送广告的成功率，广告间隔 60 秒里推送 2 次）。

39.17 HA主备环境下广告推送使用

由于图片不支持 HA 主备，存在一个问题。在主墙配置好广告推送后，当主备发生切换后由于广告图片不支持同步，导致备变主后，图片为空，只有图片名称。此时需要手动删除广告对象里图片并且重新上传图片，广告功能才可使用。

39.18 广告图片展示时间

每张图片默认展示 3 秒在加上 1 秒缓冲就是 4 秒，最多展示 4 张图片也就是 $4 \times 3 + 1$ 一共 13 秒。

39.19 广告设置白名单规格

广告推送白名单（只有命令行）。支持域名白名单（针对目的域名规格 256 条）；支持基于源地址对象的广告白名单（规格 256 条）。

39.20 广告策略匹配顺序

策略匹配顺序从上向下，如果上面策略匹配到的话，下面策略就不会在匹配。

39.21 广告策略里启用按钮和推送按钮的作用

广告策略里启用禁用是跳过当前这条配置；动作不推送，相当于命中这一条策略截止不继续往下匹配。不启用还得往下匹配。

39.22 广告对象图片上传大小

每张图片上传大小最大是 2M。

39.23 手机端广告对象限制

广告策略配置多个广告对象时。Pc 端广告展示全部生效，移动端只生效一个，广告图片随机展示。

39.24 Edge浏览器不支持广告推送

由于 edge 浏览器框架跨域不支持广告推送。

39.25 推送广告网站类型

目前只支持 HTTP 网站弹送广告，不支持 HTTPS 网站弹送广告。

39.26 广告对象里图片不能全部删除

广告对象里图片需要删除替换时，当只有一张图片时不能删除，需要先添加新的图片上传后，才能删除需要删除的图片。

39.27 今日头条app不推送广告

华为手机今日头条 app 的链接打开后广告会一直轮播无法关闭，原因是 app 与广告模板不兼容，不支持推送广告。

39.28 https网站类型使用http方式访问网页打不开

https 网站类型使用 http 方式访问网页打不开，http 页面访问被 301 重定向到 https 页面，导致无法显示。需要以 https 方式打开 https 类型的网站。

39.29 开启广告推送后访问部分网站但是过了几秒网页变成黑色

开启广告推送后访问部分网站广告可以弹出来网页也正常显示了但是过了几秒网页变成黑色，需要将该网站加入域名白名单，不推送广告。

39.30 广告推送只对域名方式的URL生效？

广告推送只对域名方式的 URL 访问生效，对 IP 方式访问的 URL 不推送广告。

40 跨三层 mac 学习 FAQ

40.1 设备学习不到交换机mac地址？

- (1) 新建交换机条目的 mac 地址是与设备相连的交换机的地址。
- (2) 设备配置的团体名需要跟交换机上的团体名一致。
- (3) 团体名不能包含中文。

40.2 新增的IP/MAC条目设备不能及时学习到该IP的数据如何处理？

开启跨三层扫描及 MAC-IP 绑定后，交换机下的新用户 IP/MAC 如果不能及时学习到，数据直接放通，在线用户列表中的 MAC 会显示成三层交换机的 MAC。

40.3 如果交换机的MAC不在扫描列表中用户数据处理流程？

如果交换机的 MAC 不在跨三层学习交换机列表中，直接拿数据 MAC 与 IP-MAC 绑定表比对。

40.4 如果交换机的MAC在扫描列表中用户数据处理流程？

如果交换机的 MAC 在跨三层学习列表中，先遍历 IPMAC 学习表获取真实 MAC，然后再与 IP-MAC 绑定表比对。

40.5 多个交换机时如何学习扫描？

配置更新时间为 30s，扫描开始后串行逐个扫描，待所有交换机扫描完毕后等待 30s 再开始下一轮扫描。

40.6 每次扫描的结果如何处理？

如果旧表中有对应 mac，则更新老化时间，如果没有，则新增。对于旧表中有但没有新学习到的 mac，等老化后删除。

40.7 跨三层MAC扫描的学习过程是什么？

学习是分两步：

- (1) snmp 协议跟交换机交互报文，来学习 IP/mac 条目，并将 IP/mac 条目存到文件中（网络好时报文交互快，学的也快）。
- (2) 从文件中读 IP/mac，进行新旧对比并更新老化时间。

40.8 快速老化机制是什么？

- (1) IPMAC 表达到 59000 条时触发快速老化，将已经老化的 IP/mac 全清掉，规格满直接丢新的条目。
- (2) 两次快速老化的时间间隔是 10 分钟。

40.9 老化定时器的工作原理？

正常情况下，全局开启跨三层扫描后启动老化定时器，30 分钟执行一次老化，然后更新定时器的时间进行下一次老化，如果条目达到 59000 条，触发定时器快速老化（记录本次快速老化的时间），然后刷新定时器为 30 分钟；当再次达到 59000 条时，if 判断当前时间-上次快速老化时间 < 10 分钟，什么都不做；否则触发定时器快速老化（记录本次快速老化的时间），然后刷新定时器为 30 分钟。

40.10 SNMP跨三层学MAC交换机规格是多大？

64，最多可以添加 64 个交换机。

41 防共享 FAQ

41.1 防共享终端显示与实际终端型号不一致？

同一个小米手机会带多个终端型号：如 MI2 会同时带 MI2、MI2S 的终端标识，终端类型会显示成先识别的终端标识，这样就可能会把 MI2 识别成 MI2S。

41.2 一个热点下多台小米手机未识别出是共享终端？

同一个小米手机会带多个终端型号：如 MI2 会同时带 MI2、MI2S 的终端标识，为防止误识别，小米手机型号不能作为用户唯一的标识。

41.3 HA环境防共享监控用户列表不能同步到备设备？

目前暂不支持防共享监控用户列表 HA 主备同步，主备切换后需要重新检测共享终端。

41.4 阻断提示中<frozen-time>单位如何处理？

阻断提示中<frozen-time>的单位是动态显示的，大于 1 分钟时会自动以分钟为单位，小于 1 分钟时会自动以秒为单位。

42 认证策略 FAQ

42.1 认证策略支持配置哪几种认证方式？

支持本地认证、短信认证、微信认证、免认证、Portal server 认证、AD 域单点登录、混合认证。

42.2 混合认证支持哪几种认证方式？

支持本地认证、短信认证、微信认证、免认证中一种或多种认证方式组合。

43 微信认证 FAQ

43.1 为什么认证时无法重定向到认证页面？

- (1) 首先查看 ipv4 策略是否将此数据包拒绝；
- (2) 查看 ACG 设备路由是否正确；
- (3) 查看用户策略是否正确，移动端或 PC 上网时是否匹配到此用户策略。

43.2 苹果手机无法自动弹出portal?

- (1) 首先查看 ipv4 策略是否将此数据包拒绝;
- (2) 查看 ACG 设备路由是否正确;
- (3) 查看用户策略是否正确, iPhone 是否匹配到此用户策略。

43.3 移动端弹出portal, 并点击一键微信连wifi后, 认证失败, 如何定位认证失败原因, 并及时修改?

- (1) 查看微信认证配置中应用 ID 是否与微信公众平台开发者中心的开发者 ID 中的 AppId 一致;
- (2) 查看微信认证配置中门店 ID 是否与微信公众平台开发者中心的设备所在门店 ID 一致;
- (3) 查看微信认证配置中 Secretkey 是否与微信公众平台开发者中心的 Secretkey 项一致;
- (4) 由于微信公众平台一个门店下所有 SSID 的 Secretkey 都一样, 所以设备侧 SSID 一定要与公众平台上的 SSID 保持一致, 否则需要保证微信公众平台上所需连接的 ssid 排列在最后;
- (5) 查看微信认证配置中其他参数是否正确。

43.4 若环境中无线路由器为cisco无线路由器, 且支持2.4G和5G信号, 假设ssid分别为cisco与cisco-5G, 此时应该连接哪个ssid?

- (1) 若微信配置与微信公众平台注册时设置 WIFI 名称均为 2.4G 信号的 ssid 即 cisco, 那么微信认证时应该连接 ssid 为 cisco;
- (2) 若微信配置与微信公众平台注册时设置 WIFI 名称均为 5G 信号的 ssid 即 cisco-5G, 那么微信认证时应该连接 ssid 为 cisco-5G;
- (3) 两者不能同时使用。

43.5 部分安卓手机弹出portal页面, 点击一键微信连WIFI后, 页面无反应或者会有提示信息“该浏览器不支持自动跳转微信请手动打开微信”, 应如何解决?

此时可以更换浏览器尝试。

43.6 微信认证页面配置是否支持HA检查?

不支持。

43.7 微信认证用户是否支持HA主备、HA主主同步?

不支持。

43.8 若一台ACG下挂两台AP, AP1有在微信公众平台上注册, 而AP2没有注册; 此时ACG上微信认证策略为全any时, 若用户连接AP2的ssid时,

不能正常认证成功，只有连接AP1的ssid时才能正常认证成功；此时如何满足此类组网？

可以将用户认证策略具体化，比如 AP1 的用户需要进行微信认证，则将源地址设置为 AP1 的 DHCP 地址池；这样避免的连接 AP2 的用户走微信认证策略。

43.9 微信认证成功后，在用户信息中心中查看微信图像没有加载成功，如何定位？

- (1) 查看 ACG 是否配置 DNS Server；
- (2) 查看 ACG 是否开启了 DNS 代理功能。

43.10 微信认证不支持双频AP的两个信号同时接入？

微信连 wifi 不能区分双频 AP 两个信号共用 DHCP 同时接入，设备无法区分 SSID，只能通过 IP 区分，若两个 SSID 使用不同的 DHCP 地址段可通过 IP 来区分。

43.11 微信认证单台设备下支持多个个SSID？

单台设备下只能支持一个 SSID。

43.12 微信认证是否支持HTTPs弹portal？

支持 HTTPS 弹 portal 。

43.13 微信认证有些安卓手机扫码连接wifi后出现网络连接失败现象？

安卓手机扫码后手机上会显示商户对应的 SSID，点击立即连接，完成手机自动连接商户对应的 SSID，之后“出现网络连接失败现象”，即使重新连接也不能成功，因为微信扫码只是实现了自动连接 SSID 的功能，边上 SSID 后，手机会通过微信触发 https 流量，但此时由于用户通过认证，所以流量会被设备阻断，设备上放通微信流量的报文时机是在 portal 页面上点击一键唤醒微信的按钮之后才会放通一分钟。再加上设备无法对微信的 https 流量进行重定向，所以无法自动弹 portal。此时需要手动打开浏览器触发弹 portal 完成接下来的认证流程，实现上网。

43.14 PC推荐浏览器？

PC 端进行微信认证时的浏览器支持 IE9 及以上，火狐、谷歌浏览器，对于火狐浏览器网银模式不支持，请务必使用网银模式。

43.15 移动终端推荐浏览器？

移动终端浏览器推荐：

手机品牌	推荐浏览器
iPhone	QQ浏览器、百度浏览器
ipad	QQ浏览器、百度浏览器
三星	QQ浏览器、百度浏览器
华为	QQ浏览器、百度浏览器
oppo	QQ浏览器、百度浏览器
小米	QQ浏览器、百度浏览器
魅族	QQ浏览器、百度浏览器

43.16 设备上的WiFi名称不支持中文？

设备上的 wifi 名称(SSID)建议不要使用中文、如果使用中文可能会存在兼容性问题出现乱码或无法连接的问题。具体请参考微信公众平台说明：<https://mp.weixin.qq.com/wiki>，附截图说明如下。

字段说明：

字段	是否必填	说明
shop_id	是	门店ID
old_ssid	是	
ssid	是	无线网络设备的ssid。32个字符以内；ssid支持中文，但可能因设备兼容性问题导致显示乱码，或无法连接等问题，相关风险自行承担！当门店下是portal型设备时，ssid必填；当门店下是密码型设备时，ssid选填，且ssid和密码必须有一个以大写字母“W X”开头

43.17 微信连wifi未认证情况下用户微信能收发消息？

为了实现微信内置浏览器弹 Portal，默认放通了 dns.weixin.qq.com（DNS 报文会封装到这个域名的报文中）、short.weixin.qq.com（获取用户 OpenId）的流量，不认证的情况下微信能正常收发消息，因为微信收发消息被封装在 short.weixin.qq.com 的报文中了。

43.18 微信内置浏览器访问部分公众号不能弹出Portal页面？

微信内置浏览器中大部分应用都部署在微信服务器上，访问时报文已被微信私有协议 mmtls 加密，导致不能弹 portal，此类 url host 一般是 <http://mp.weixin.qq.com>。

例如：<http://mp.weixin.qq.com/s/YOkQ0zn7fYi35KK8m3Gw8w>，经测试统计这类应用的比例高达40%左右，另外还包含以下情况不能弹 Portal：

(1) 微信内置浏览器中的 https 页面不支持弹 portal。

- (2) 部分 http 页面不能弹 portal,原因是终端建立 tcp3 次握手后,不发送 GET 请求了,与终端行为有关。
- (3) 订阅号中的应用不支持弹 portal,都是内置在微信服务器上的应用,微信不会响应 302 重定向报文。

43.19 苹果手机不能通过3G/4G实现扫码认证?

苹果手机不支持扫码认证,在微信扫码认证时,因为微信需要获取 root 权限打开手机无线,苹果手机没有开放 root 权限,安卓手机默认都开放了 root 权限。

43.20 微信连wifi强制关注功能支持订阅号吗?

强制关注支持订阅号和服务号,但强制关注所用的订阅号和服务号必须是已通过微信官方认证的,否则没有权限获取 access_token。

43.21 微信连wifi何时需要设置token-url?

在开启强制关注后,若有两个及以上门店使用同一个微信公众号,则需要搭建第三方 token 服务器,并将 token-url 设置为 token 服务器的地址,否则会导致强制关注功能异常,因为门店 ACG 网关每 105 分钟会去微信公众号更新 access-token,一旦 access-token 更新就会失效,这样就会导致同一时间总有一个门店获取关注用户列表失败的情况,设置一个 token-url 间接获取 token 就能避免这样的情况出现。

43.22 微信连wifi电脑端弹出的portal微信二维码一段时间后超时,提示:服务器繁忙请一分钟后刷新重试?

原因:微信客户端一次请求的等待时间为 10s,请确保后台认证服务器在微信客户端向 authUrl 发送请求 10s 之内返回 AC 认证结果,即 http 返回码。超过 10s 未返回认证结果将视为认证失败。

44 用户源 MAC 日志显示 FAQ

44.1 用户源MAC如何获取?

用户源 MAC 获取方式因组网环境不同会有差异:

二层组网:直接获取报文中的用户源 MAC,显示到日志中。

三层组网:不开启 SNMP 跨三层 MAC 学习功能的话,也是直接获取报文中的用户源 MAC,显示到日志中。如果开启 SNMP 跨三层 MAC 学习功能,先取报文中的源 MAC 同交换机列表中的 MAC 进行比对,如果匹配到,则到该交换机列表中获取真实的源 MAC 显示到日志中,如果没匹配到则显示报文中的源 MAC。

45 免认证 FAQ

45.1 免认证用户不需要认证账号？

免认证方式是一种支持用户自定义认证 portal 进行广告宣传，同时不需要输入账号即可实现快速上线的认证方式，可提升用户体验。用户访问网页时被重定向到已定义好的 portal 页面，点击登录按钮即可完成认证流程。

46 无感知认证 FAQ

46.1 什么是无感知认证？

用户第一次接入网络时会弹 portal 认证页面，用户按照要求输入正确的用户名及密码后完成认证并成功上线，此时设备会将该用户的 MAC 加入到无感知列表，当用户下次上线时先查无感知列表，如果用户 MAC 在无感知列表中，设备自动完成认证，将用户无感知上线，简化了认证流程，提升了用户体验。

46.2 无感知认证超时时间计算标准？

用户认证上线后，设备将该用户的 MAC 加入到无感知列表，当用户下线后，设备启动超时定时器，在超时时间范围内用户再次上网可以无感知上线，若大于超时时间，设备会将该用户 MAC 从无感知列表中删除，此后用户下次上线时需要重新输入账号密码进行认证。

46.3 无感知认证支持跨三层组网吗？

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

46.4 哪几种方式支持无感知？

本地认证、短信认证、微信认证都支持无感知。

46.5 无感知在哪些情况下生效？

- (1) 用户超时下线，并非用户自己主观行为，所以应该支持无感知，让用户没有重新认证的感觉。
- (2) 用户被管理员踢下线，证明用户存在一定的异常，针对异常用户肯定不能无感知。
- (3) 用户主动注销，证明下线是用户主观的行为，不想在不知情的情况下再次上线，所以也不能支持无感知。

通过如下命令检查用户上线后 MAC 是否被加入到无感知记录表中：

- display user-waa local-waa 查看本地认证无感记录表。

- display user-waa sms-waa 查看短信认证无感知记录表。
- display user-waa wechat-waa 查看微信认证无感知记录表。

47 混合认证 FAQ

47.1 什么是混合认证？

混合认证就是在用户认证时提供多种认证方式供用户选择，用户可根据需要灵活切换认证方式，混合认证目前支持微信认证、短信认证、本地认证、免认证四种认证方式。

47.2 混合认证能选择单一的认证方式吗？

在混合认证里既可以选择单一的认证方式，同时也选择 1 种至 4 种的认证方式。

47.3 混合认证的模板和其他认证一样吗？

不一样，混合认证的模板是轮播模板，支持广告轮播。然而其他认证模板是默认模板。

48 短信认证 FAQ

48.1 用户使用浏览器A获取短信验证码，在浏览器B上输入手机号和验证码，是否能短信认证成功？

无法认证成功，短信认证与浏览器是绑定的。

48.2 设备导出设备配置，是否包含短信认证配置？

不包含短信认证的配置，由于短信认证没有命令行，所以导出的设备配置不包含短信认证配置。

48.3 双机主备环境，主设备配置短信认证，备设备是否同步短信认证的配置？

不同步。

49 微信白名单 FAQ

49.1 微信白名单是什么？

微信白名单就是认证方式选择为微信认证，配置微信白名单以后，可以免认证上网。

49.2 微信白名单和全局白名单有什么不同？

全局白名单针对的是所有的认证方式，而微信白名单针对的是微信认证这一认证方式。

49.3 微信白名单对混合认证中的微信认证方式生效吗？

微信白名单在混合认证方式中不生效，因为混合认证方式会弹混合认证风格的认证界面，支持认证方式手动切换，如果混合认证中包含微信认证方式，弹 portal 之前无法确认用户是否会选择微信认证，即使用户选择了微信认证，也无法匹配白名单了，因为白名单的流程是在认证弹 portal 之前，弹 portal 后再命中白名单违背了白名单的设计初衷，即配置白名单的用户是不会弹 portal 的。

50 https 弹 portal

50.1 什么是https弹portal？

https 弹 portal 是指终端访问 https 的网站认证上网，https 网站能弹出认证页面 portal。

50.2 安卓手机https弹portal警告非安全怎么办？

由于 https 是加密的，访问 https 页面就需要 ssl 证书，所以手机访问部分 https 网页的时候，会弹出一个警告信息，部分 https 网站提示完可以继续访问，但是也有部分网站直接禁止继续访问该页面。这时候可以换一个浏览器或者换一个 https 网页重新访问。

50.3 https弹出portal以后没有认证为什么可以正常打开网页？

因为微信认证中，由于用户与微信服务器的交互都是 https 加密的，对于 PC 端而言，打开 https 网页弹出 portal 以后，流量会自动放通一分钟，以使用户能与微信服务器通信完成交互生成二维码信息，对于移动终端而言，弹 portal 后点击“一键唤醒微信连 wifi”的按钮后流量会自动放通一分钟以便正常唤醒微信，完成接下来的认证流程。

50.4 https弹portal支持所有https域名url吗？

由于不同的浏览器对一些流行的购物网站（如京东、淘宝）或门户网站（百度）证书安全级别有强制保护检查，浏览器检测到 https 弹 portal 的行为证书不合法，则不会继续访问 portal 页面，导致无法弹 portal，此外对于银行 https 网站都无法实现弹 portal。

IE11 浏览器有合法证书强制检查，不信任的证书网站不允许用户继续浏览，进行强制保护，导致设备无法对 https 网站弹 portal。

50.5 为什么在浏览器上通过导航网站访问https类型网站时没有弹portal?

通过门户网站间接访问的其它网站，由于有些网站本身点击跳转时不是访问的目的网站的真实网址，而是还会通过门户网站提供的一个特殊的地址访问后再重定向到最终想要访问的网站的真实地址。对于这种 https 加密的方式进行访问的网址不支持 https 弹 portal 认证。

50.6 怎样能使https类型的网站弹portal?

配置本地 web 认证或者其它认证方式，保证认证地址能进行正确认证，就能在访问 https 类型网站时弹出 portal。

50.7 浏览器多次访问https页面，会出现弹出认证页面很慢的情况?

这个现象是由于浏览器针对不安全页面进行的一个安全提示，属于浏览器的一个易用性功能，因为显示等待一段时间，目的就是提示用户，这个是不安全的。用户不选的话，等待一会浏览器还会自动前往。这个属于浏览器的易用性考虑。

50.8 访问https类型网站时有的浏览器无法弹出portal认证界面?

是由于浏览器本身的拦截造成的，由于浏览器本身的拦截，请求并没有发起，而是直接被浏览器处理掉了。

50.9 默认不使能https弹portal功能?

https 弹 Portal 功能非常耗性能，在用户量较大时会导致 Portal 页面弹不出来，影响用户认证，所以默认情况下不使能，并且不建议在大流量场景下开启此功能，使能命令 **user-policy https-portal enable**。

51 伪 Portal 抑制 FAQ

51.1 伪portal抑制原理是什么?

伪 portal 抑制使用的是 refresh 脚本方式进行重定向，客户端收到重定向报文后需要解析脚本成功后才能访问 Portal 页面，与 302 重定向不一样，因为一般的软件不会解析脚本，所以就不会发起访问 Portal 的请求，在一定程度上就减轻了无效的访问对设备造成的压力。

51.2 refresh重定向是一定起作用吗?

不能排除部分软件可以识别 refresh。这个功能是能在趋势上减少请求量，不能保证所有软件都会起作用。

51.3 refresh重定向能有效抑制所有的软件吗？

refresh 重定向不一定能有效抑制所有的软件，只是说会减少一部分不会识别的 refresh 脚本的软件。

52 强制关注 FAQ

52.1 什么是强制关注？

微信认证强制关注就是用户需要关注客户公众号才能在认证成功后持续稳定上网，否则会在 5 分钟内被设备踢下线。

52.2 第一次上线是否需要先关注公众号？

不需要，强制关注实现原理是：用户无论是否关注过公众号，均可以正常弹 portal 完成微信认证，当用户通过微信认证上线后，设备会定期（5 分钟一次）与微信公众平台交互获取对应公众号关注列表，如果用户上线后不关注公众号，关注列表中没有此用户，那么设备会把此用户踢下线，防止用户蹭网。所以如果在微信认证成功后要想持续稳定上网，建议在完成认证流程后点击关注公众号。

53 认证模板设置 FAQ

53.1 什么是认证模板设置？

认证模板设置包含本地认证、微信认证、短信认证、免认证的弹出 portal 页面的风格自定义，同时增加了轮播模板，可用于以上四种认证方式，即每一种认证方式都包含两套模板：默认模板以及轮播模板，轮播模板支持 3 张背景图片循环播放。

53.2 认证模板预览有认证方式切换功能？

认证模板预览支持认证方式切换效果的展示，但目前尚不支持此功能。

54 策略查找 FAQ

54.1 策略查找支持哪几个维度？

策略查找界面提供基于以下维度的搜索功能：

- 策略 ID：精确匹配
- 源地址：地址对象精确匹配，IP 地址模糊匹配
- 入接口（源区域）：精确匹配，且该选项是唯一性的
- 用户：精确匹配，该选项是多选项

- 目的地址：地址对象精确匹配，IP 地址模糊匹配
- 出接口（目的区域）：精确匹配，且该选项是唯一性的
- 应用：精确匹配，该选项是多选项
- 服务：精确匹配，该选项是多选项

以上搜索中多选条件项，每项最多可以同时选择 8 个对象。

同一个条件内部是或的关系，只要包含其中一个对象即可。条件与条件之间是与的关系，必须全部满足才可以搜索成功。

55 地址本域名 FAQ

55.1 什么是地址本域名？

地址本域名是指在地址对象中支持添加域名方式的对象，并支持在其他策略中引用。

55.2 地址本域名在策略中引用后不生效？

地址本域名支持添加域名形式的地址对象，设备会将域名解析成对应的 IP 地址，在策略匹配过程中实际还是直接匹配的 IP，如果发现策略命中不生效，检查设备是否配置了 DNS，以及查看域名是否成功解析成了 IP 地址。

56 NAT44 FAQ

56.1 NAT44支持端口利用吗？

NAT44 支持端口复用，只要一条流的 DIP、Dport、portocol 有一个参数不一样就可以转化成相同的源端口。

56.2 NAT44端口分配规则？

NAT44 端口分配是随机的，从尚未使用的端口号中随机选择一个进行转化。

57 4G 上网卡 FAQ

57.1 目前支持哪些型号4G上网卡？

目前仅支持华为 E3372 联通版本的 4G 网卡。

58 PPPOE 拨号 FAQ

58.1 设备CPU100%情况下停流后仍然不能成功拨号？

设备在 CPU100%的情况下会出现大量丢包，拨号报文发不出去，在连续发 10 个包后，没有响应，会导致 lcp down，然后报 close 事件，根据 PPP 状态机，PPP 切换到 closing 状态。

然后超时，收到 To-事件，状态切换到 closed 状态，此时收到 server 端的 Configure-Request packets 时，会发送一个 Terminate-Ack。收到 server 端的 Terminate-Acks 被静静的丢弃，以防止造成循环。

不再主动发包，等待 up 事件触发，所以需要接口 shutdown、no shutdown。

59 新版本链路负载均衡 FAQ

59.1 负载均衡配置规格？

- (1) 负载均衡出接口配置规格 32。
- (2) 单独一个出接口允许添加健康检查的个数规格 8。
- (3) 负载均衡策略配置规格 32。
- (4) 单独一条负载均衡策略可以添加的出接口（包括出接口组）规格 8。
- (5) 出接口组中可以添加的出接口的规格 4。
- (6) 免负载地址可以添加的地址对象（包括地址对象组）规格 8。
- (7) 加入到负载均衡组中的接口不能再加入到桥口或聚合口和 HA 心跳口。

59.2 负载均衡支持的负载方式？

目前支持基于权重负载和优先级负载两种方式。

59.3 权重的负载方式使用的算法？

选路的规则是按照链接哈希，结合权重完成选路，同一链接的所有转发要求使用同一个接口完成。

关于父子链接的应用：sip, h323, pptp, ftp, tftp 等要求主从链接必须使用同一个接口完成转发，使用源地址 hash，这样就可以保证同一源地址的所有请求使用唯一接口完成转发。

59.4 权重的负载使用条件？

- (1) 权重的范围 1-100。
- (2) 出接口状态为 up 的接口能够参与权重比计算。

59.5 优先级定义

负载均衡策略添加的出接口，按照由上到下的匹配顺序，进行转发。

这里的优先级需要明确，最优链路出现故障，则使用第二优先级的链路转发，一旦最优链路恢复，则新的链接使用最优链路完成转发，旧得连接在原有的接口上维护。

59.6 负载方式为优先级的使用条件？

- (1) 优先级的匹配顺序是由上到下。
- (2) 最优链路出现故障，则使用第二优先级的链路转发，一旦最优链路恢复，则新的链接使用最优链路完成转发，旧得连接在原有的接口上维护。
- (3) 优先级可以通过上下箭头进行调整，按照调整后优先级完成转发。

59.7 会话保持使用说明？

新版本的会话保持功能，使用源地址 hash，这样就可以保证同一源地址的所有请求使用唯一接口完成转发，如 FTP 控制流和数据流走同一链路，同一用户的请求能持续在同一个链路进行负载，避免网银等业务不可用。

59.8 过载保护使用说明？

新版本暂时不支持过载保护功能。

59.9 健康检查

- (1) 链路负载出接口，添加健康检查（健康检查地址需要配置可达地址）。
- (2) 健康检查支持协议：暂时仅支持 ICMP 检测。
- (3) 链路负载均衡出接口，最多添加 8 个健康检查条目，8 个检查条目，只要有任何一个检测失败，认为该出接口健康检测失败，该接口状态为不可用。

59.10 链路负载均衡出接口配置说明？

- (1) 出接口为三层口静态 ip 的接口，必须配置下一跳地址。
- (2) 出接口为 pppoe, dhcp, tunnel 接口，不需要手动配置下一跳地址。

59.11 免负载均衡地址使用说明？

- (1) 默认配置排除设备的直连网段，也就是说直连网段的地址访问外网，不需要进入负载均衡流程。
- (2) 选中的免负载均衡地址访问外网，不需要进入负载均衡流程。

59.12 负载均衡策略匹配条件-匹配应用使用说明？

新版本暂时不支持匹配应用的负载均衡。

59.13 负载均衡，策略路由，静态路由匹配顺序？

首先匹配策略路由，未匹配上策略路由匹配负载均衡策略，均为匹配上，匹配静态路由。

59.14 负载均衡流量匹配说明？

- (1) 链路负载均衡本身的匹配顺序，先匹配免负载均衡地址，负载均衡策略由上到下匹配。
- (2) 负载均衡能够匹配正向发送的流量，无法匹配反向进入设备的流量（配置负载均衡策略，同样要配置相应的默认路由，保证目的 nat 功能可用）。

59.15 负载均衡的ISP地址配置说明？

- (1) ISP 地址的导入命令：**copy ftp** 服务器 ip 导入的 isp 地址库名称 **isp-address**
- (2) isp 地址导出命令行：**export isp-address by ftp** 服务器地址
- (3) ISP 地址导入后需要执行 **isp address update**，导入的 isp 地址生效
- (4) ISP 地址导入后需要执行 **isp address creat**，isp 地址生效
- (5) ISP 地址删除命令，**isp address delete**

60 用户/用户组优化 FAQ

60.1 用户/用户组的规格？

- (1) 用户的规格是根据不同设备型号（不同的内存来决定的，范围是 4096-32768）。
- (2) 用户组的规格所有设备相同，均为 1024。

60.2 用户页面能否完整显示8个所属用户组？

用户页面能够完整显示前 3 个用户组，剩余的用户组通过省略号代替，但是会显示具体的所属用户组个数。

60.3 用户组引用用户的个数规格？

用户组中引用用户的规格为 2048，当所选用户超过 2048 个，无法全选移动到指定用户组。

60.4 用户/用户组的移动？

用户支持批量移动，用户组不支持批量移动，仅支持单独移动。

60.5 用户/用户组的导入导出？

- (1) 用户导入支持追加导入，不支持覆盖导入，如导入文件中的用户与系统中已存在用户名称相同，则导入失败。回退导入操作。
- (2) 导出：导出所有用户和用户组。
- (3) 导入/导出的文件后缀格式（.csv）。

61 LDAP 服务器同步 FAQ

61.1 异常AD域用户名同步到设备的处理

LDAP 服务器用户名长度大于 63 字符后同步到设备用户名会截断成 63 字符。

61.2 LDAP服务器同步端口？

LDAP 服务器同步目前支持 389 明文传输，不支持 636 密文传输（加密跟服务器交互不了 身份验证不了）。

61.3 LDAP组的作用？

在用户管理>全局配置>第三方 LDAP 认证处，选择 ldap 组统一认证。

61.4 LDAP绑定方式对同步用户的影响？

Windows AD 域不支持匿名同步用户，OpenLdap 服务器支持匿名同步 499 个用户。

61.5 LDAP同步用户的限制？

AD 或者 Openldap 服务器上用户名超长(大于 63 字符)；（汉字数字字母以及@._-()[]以外的特殊字符）；单 OU 下大于 2048 个用户的。

61.6 LDAP BaseDN写法？

LDAP BaseDN 如果写根 OU 的话，同步 LDAP 服务器的时候会把根 OU 下的所有子 OU 以及用户全部同步下来。

61.7 被策略引用的远端用户被删除时，策略的变化

远端用户删除后重新同步 ldap 组后，远端被删除的用户移除用户组，本地用户没被删除，不会影响到策略。

61.8 使用LDAP用户认证通过后，在服务器删除认证用户并在设备上同步该OU？

- (1) 由于远端用户认证未下线所以本地即使没有该认证用户也不影响下联 pc 上网。
- (2) 当远端 pc 认证用户下线后重新使用被删除的用户进行认证是提示用户不存在。

61.9 HA主备环境下LDAP同步支持？

HA 主备环境配置不会比较 ldap 同步下来的用户。

61.10 IPsec使用LDAP认证？

IPsec条件下使用LDAP认证时，IPsec认证使用用户名密码认证后，会从本地查找该用户名用户，若该用户不存在，则不会添加该用户到认证用户组。所以若使用该方式认证，需保证本地存在该用户。

61.11 LDAP自动时间？

LDAP定时同步设定的时间范围为0-23，例如：23，所代表的含义是时间整点为23点的一个小时时间段内均为自动同步的有效时间，即23:00-23:59为自动同步有效时间。

62 端口镜像FAQ

62.1 端口镜像规则有哪些配置限制

- (1) 接口已经作为镜像规则源接口时不可再配置为其它规则的监控接口；
- (2) 接口已经作为镜像规则监控接口时不可再配置为其它规则的源接口；
- (3) 源接口和监控接口不能是同一个物理接口，要么配置为源接口，要么配置为监控接口，不能同时配置；
- (4) 管理口以及旁路接口不可配置为监控接口；
- (5) 在线业务口不可配置为监控接口（在线业务口即为现网在跑正常业务的物理接口）。

62.2 配置端口镜像后并未镜像出业务流量

- (1) 查看接口是否up，只有镜像接口up时才进行端口流量镜像，否则不进行流量镜像；
- (2) 设备packet buffer数量使用率超过3/4，可通过**display statistics fpa**命令中PKI_POOL一行查看当前的使用情况，如果正常业务流量的packet buffer数量使用率超过3/4则镜像功能失效，不再镜像业务流量。

62.3 配置端口镜像后只镜像出了部分业务流量

设备packet buffer数量使用率超过3/4，可通过**display statistics fpa**命令中PKI_POOL一行查看当前的使用情况，如果正常业务流量的packet buffer数量使用率未超过3/4，但匹配镜像功能后超过3/4，则会出现只镜像出部分业务流量的现象。

62.4 如何配置将多个接口的流量镜像到同一个监控接口

需要配置多条端口镜像规则，每条规则配置不同的源端口镜像到同一个监控接口，目前端口镜像规则的源接口、监控接口只允许配置一个物理接口，无法配置多个物理接口。

62.5 是否支持远端镜像功能

不支持，由于 ACG 仅仅支持单台模式，因此仅仅支持本地镜像，而不支持远端镜像。

62.6 使用设备上的抓包工具是否能够抓取到监控接口镜像过来的业务报文

不能。

62.7 如何查看镜像功能是否生效

使用 **display statistics phy-interface** 命令或在 web 页面查看监控接口的发送的流量大小是否等于端口镜像规则源接口所配置镜像方向的流量的大小。

62.8 是否可以配置将万兆口流量镜像到千兆口或千兆口流量镜像到百兆口

可以，但是镜像前要保证被镜像的源接口的流量小于监控接口真实的物理带宽，否则监控接口发送报文出现拥塞，造成系统大量丢包，影响报文正常转发，造成业务中断，因此建议使用时配置低带宽向高带宽接口镜像，尽量不要高带宽往低带宽接口镜像。

63 解密策略 FAQ

63.1 设备开启https解密后，电脑必须要安装设备上导出的证书吗？

电脑必须要安装，如不安装会出现浏览器提示证书不合法无法访问的情况。

63.2 电脑端证书如何导入？

电脑端需要安装证书在浏览器的受信任根目录下，具体导入过程见【证书导入文档】。

63.3 证书的有效期是否影响解密？

证书有始发日期和结束日期，当导入证书以后，用户电脑当前时间小于证书的始发日期会导致证书无法使用。用户电脑当前时间大于证书的结束日期也会导致证书无法使用。

63.4 设备DNS设置全局模式时，为什么显示的证书不是颁发证书？

当设备 DNS 设置成全局模式时，用户电脑的 DNS 需要指向设备的入接口，以保证 DNS 过设备，解密策略才能生效。若 DNS 不经过设备的话，解密策略不生效。

63.5 为什么安装证书以后，chrome浏览器访问12306网站显示非安全连接？

Chrome 浏览器原本打开的 12306 就是报非安全连接，并且 Chrome 和 Firefox 浏览器把全部 http 视为非安全连接。

63.6 两台防火墙串联，用户电脑应该导入哪一台的证书？

如果两台防火墙串联（PC-ACG1-ACG2），ACG1 证书为 mm.cer，ACG2 证书为 https.cer，用户电脑应该导入 ACG1 的证书 mm.cer。

63.7 防火墙的证书一定要和用户导入证书一致吗？

防火墙的证书必须和用户导入的证书一致，否则浏览器依然显示证书非安全。

63.8 防火墙下连的无线设备，手机端也需要导入证书吗？怎么导入？

手机端（Android/ios）都需要导入证书，如果不导入，手机端访问网址、发送邮件、升级系统都会报非安全连接或者验证错误。

63.9 所有邮箱客户端都支持审计吗？

不是，有些邮箱客户端（网易邮箱大师/闪电邮）的 smtp 是使用的 TLS 加密，TLS 加密不支持解密。

63.10 配置Https解密后百度页面打不开？

广告对于使用了 HSTS 技术的网站，配置 https 解密后会出现大家概率打不开的情况，请将该域名排除。

63.11 https解密审计对移动终端生效吗？

支持对安卓、IOS 移动终端的 https 审计，但必须导入证书，证书导入方法参考解密策略典配文档，部分移动终端自带浏览器访问页面时会报证书不安全的提示。

63.12 https解密策略开启后，移动终端APP无法访问网络？

由于部分 APP 对证书有高安全级别的检验，移动终端导入的证书就会检验不通过，导致无法访问，如果出现此情况，则在解密策略中排除 APP 应用服务器的 IP 或者关闭解密策略。

64 DDNS 功能 FAQ

64.1 DDNS规格限制

DDNS 功能的规格限制是以配置的账户名的数量做限制的，目前支持配置 10 个不同的账户名，由于每个 ddns 条目只能配置一个账户，且不同的 ddns 条目不允许配置相同的账户名，因此 ddns 功能支持配置的条目也是 10 条。

64.2 当公网口存在多个IP时使用哪个IP地址？

当外网口地址存在多个 IP 地址时，DDNS 更新时使用主地址进行更新，不会使用从地址，不支持指定某个特定的 IP 地址进行更新。

64.3 DDNS配置了更新某一特定域名，为什么此账户下的所有域名地址都进行了更新？

由于花生壳厂商不支持对指定的特定域名进行更新，而是会更新此账户下的所有域名导致，后续会进行优化，嵌入支持其它服务商。

64.4 DDNS与DNS功能模块功能关系？

这是两个完全独立的功能，分别针对不同的场景，并没有直接关系；但是在 DDNS 功能使用时需要先解析 DDNS 服务商的域名地址进行注册和认证授权，因此需要设备配置有 DNS 服务器，DDNS 才能够正常使用，DNS 服务器可以手工配置，也可以通过在 DHCP 或 PPPoe 接口动态获取。

65 DNS-DNAT 功能 FAQ

65.1 DNS-DNAT规格

由于设备支持配置 32 个链路负载出接口，每条链路负载出接口均支持配置 dns-dnat 功能，因此 dns-dnat 规格与链路负载出接口一致。

65.2 如果设备同时开启dns透明代理和dns-dant功能，DNS报文如何处理？

DNS 透明代理功能优先处理 DNS 报文，DNS 报文不会在进 DNS-DNAT 流程处理。

65.3 DNS-DNAT探测功能是什么？

DNS-DNAT 的探测功能在配置 DNS-DNA 后就会默认开启，设备主动往主、备 DNS 服务器发送域名 `www.baidu.com` 的 dns 请求报文，每 10s 发送一次，重试次数为 3 次，即如果连续三次未收到 DNS 服务器的 dns 恢复报文则认为此 DNS 服务器故障。

65.4 如何查看DNS服务器是否正常状态？

在 web 管理页面，网络配置>负载聚合>负载均衡出接口配置页面查看，如果 DNS 服务器探测失效时，DNS 服务器的显示将变为红色字体，将鼠标放在 dns 服务器显示 IP 处，会有弹出框显示“此 dns 服务器探测失败，为故障不可用状态”；在 cli 下可通过命令行 **display lb-policy wans interface state** 进行查看；在 dns server 后面会显示当前 dns 服务器成功还是失败，并且后面会有相应的标识，各状态标识含义如下：

- 0x00 表示均不健康
- 0x01 表示主是健康的
- 0x02 表示备是健康的
- 0x03 表示均健康

66 多配置管理功能 FAQ

66.1 配置文件限制

支持保存、导出、导入配置文件的格式为.cfg 格式（导入时支持 web 页面导出的.data 加密格式的配置文件），只支持保存配置文件的数量为 6 个，所有配置文件占总存储大小空间为 200M。

66.2 配置文件保存在哪？清除配置重启时是否会清除掉配置文件？

配置文件保存在 CF 卡中，当 CF 卡空间不足以保存配置文件时会进行提示；使用 `erase startup-config` 命令清除所有配置重启后不会清除掉保存的配置文件。

66.3 如何查看我保存的配置文件？

可使用 `display config-list` 命令查看当前设备保存的配置文件，并且会显示配置文件保存的时间点，顺序按照时间点从最新到最老进行显示排列。

66.4 在使用ftp方式导出配置文件时为什么配置了服务器地址和文件名称后面还提示输入服务器地址？

在命令行下使用 `copy config test.cfg ftp 192.168.2.120 test.cfg` 导出配置文件时，输入“?”时后面仍会提示输入 FTP 服务器的地址。如下所示：

```
A.B.C.D Address of ftp server
# copy config test.cfg ftp 192.168.2.120 test.cfg
<CR>
A.B.C.D Address of ftp server
# copy config test.cfg ftp 192.168.2.120 test.cfg
```

这是由于 FTP 导出配置文件的注册命令是这样 2 条命令：“**copy config LocalFile ftp USERNAME PASSWD A.B.C.D RemoteFile**”，“**copy config LocalFile ftp A.B.C.D RemoteFile**”，“**copy config test.cfg ftp 192.168.2.120 test.cfg**”执行的命令给识别为第一条命令了，把 IP 地址作为 USERNAME 来使用，所以导致输入？仍会提示输入 FTP 服务器地址。FTP 导出命令是分为 2 个命令注册的，一个是匿名用户，一个需要输入用户名/密码；在输入 IP 地址和文件名称时无法区分是否是用户名、密码还是服务器、文件名称。

67 Portal 逃生 FAQ

67.1 设备portal逃生用户根据设备内存大小来设置存储规格？

1G 内存设备存储规格为 1000；
2G 内存设备存储规格为 5000；
4G 内存设备（含小于 8G 设备）存储规格为 1W；
8G 及超 8G 内存设备规格为 2W。

67.2 portal逃生功能开启，全局逃生模式的含义？

要求在逃生时所有用户均可上网、逃生结束后未认证用户均需认证。也就意味着，在逃生期间在线用户不发生变动。

67.3 portal逃生功能开启，已认证用户逃生模式的含义？

要求在逃生时在线用户和 mac 地址在已认证用户列表里的用户可以上网，其它用户不能上网。

67.4 portal逃生存储用户数达到规格时设备如何更新？

认证用户有保存用户数的规格限制，当存储用户数达到规格时，优先删除最久没有流量的用户。

67.5 portal逃生功能什么时候生效？

地址探测模块负责向指定的 Portal 服务器或着内容平台发送探测报文。当 Track 状态变更时，向 Portal 逃生模块通知 Track 的状态，当 track 状态为不可达，portal 逃生功能开始生效（探测次数和间隔时间是根据地址探测的配置来决定）。

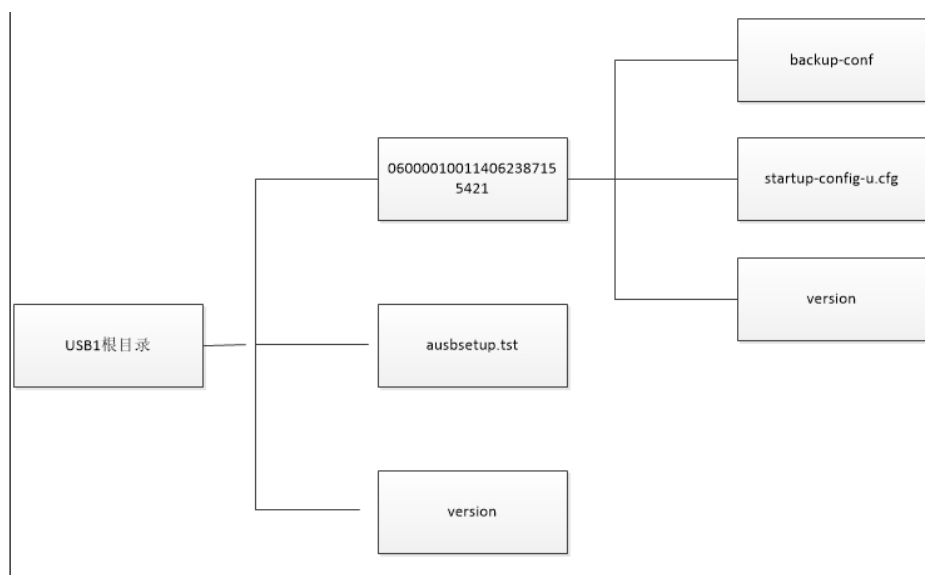
68 零配置上线 FAQ

68.1 零配置启动盘格式？

零配置启动盘格式为 FAT32。

68.2 零配置启动盘文件结构？

启动盘的文件结构如下图所示：



68.3 零配置启动盘生效后能作为硬盘吗？

可以，启动成功后执行命令即可。

68.4 零配置启动盘里根目录下的version和序列号文件夹里version有什么差别？

根目录下的 **version** 是文件里，里面放置需要更换的版本文件，序列号文件里的 **version** 只是一个放置版本号和版本名称的文件。

68.5 设备运行阶段插入零配置上线U盘有影响吗？

没有影响，只有在重启的过程中生效。

68.6 零配置启动盘只能生效一次吗？

零配置启动盘启动成功后会在序列号文件夹下生成一个 **finish** 的文件。把文件删除后，还能继续生效。

68.7 零配置启动盘失败会有提示吗？

零配置启动盘启动后，不论失败或者成功，**show log debug** 即可看见日志。

68.8 零配置启动盘只能针对一台设备吗？

不是，启动盘里可支持 1024 序列号。

68.9 零配置启动盘序列号文件夹下启动配置和备份配置分别支持几个？

启动配置是一个，备份文件是三个。

69 审计日志导出 FAQ

69.1 同一设备可以同时导出多个类型日志吗？

不能，会按照操作时间顺序导出日志。

69.2 审计日志包括哪些类型？

包括应用审计日志下所包含的：IM 聊天软件日志、社区日志、搜索引擎日志、邮件日志、文件传输日志、娱乐/股票日志、其他应用日志。以及网站访问日志下所包含的：访问网站日志、恶意 URL 日志。

69.3 审计日志可导出所有时间的日志吗？

不支持一次性全部导出所有日志内容，只能按指定日期范围导出日志文件，当前支持导出“今天、近三天、近一周、近一月、近三月”。

69.4 审计日志导出支持负载内容导出吗？

不支持，比如邮件日志里的内容和附件就不支持导出。

69.5 所有设备都能导出审计日志吗？

只支持带硬盘可以访问审计日志页面的设备才具备日志导出功能。

69.6 审计日志有规格限制吗？

有，户导出的最大日志大小为 25 万左右（对应的文件大小在解压后 64M 左右，存在一些误差），因此当数据量较大时，用户选择了近三月的数据，可能只导出了几天或十几天的数据。所以导出的日志数量为导出规格的先决条件，其次才是选择的时间范围。

69.7 如果近一周审计日志的某天是没有日志，还能导出来吗？

当导出日志中某一天无日志记录时不生成该日期的空内容导出文件。

69.8 修改系统时间小于当前时间后，导出今天的审计日志实际导出出来的是其他日期的日志？

导出今天的日志系统只做了起始时间的判断，没做终止时间的限制，如果人为修改了系统时间，就会导出比当天时间大的日志。影响很小，基本不影响现网环境使用，只要保证系统时间是对的就行，对于设备来说，当天只要下一个起始时间就能导出正确的日志来。

70 业务告警 FAQ

70.1 配置完邮箱服务器怎么关闭该功能？

告警事件的全局开关就是“启用事件告警”，取消勾选后整个功能处于关闭状态。

70.2 会话警告阈值规格是按照什么统计的？

会话警告阈值规格是按照设备的会话规格统计的，例如设备会话限制 30W，会话警告阈值就最大值就是 30W 条。

70.3 邮箱服务器发送地址用户密码是指邮箱登录密码吗？

一般情况下，用户密码是指发送地址的邮箱登录密码，但是因为部分邮箱设置了第三方授权登录码的，密码这块就需要填写授权码。

70.4 配置了邮箱服务器但是没有收到邮件？

首先检查是否配置 DNS，确认与邮箱服务器正常连接后，可以点击测试邮箱有效性，如果收到邮件证明配置填写无误，如果未收到邮件，则是配置填写有错误。

70.5 邮箱服务器重置配置没有清空？

重置会回到前一次的配置，并不是清空配置。

70.6 告警日志弹窗会在任何界面弹出吗？

不会，只有在设备主页系统状态页面会弹窗告警。

70.7 告警日志记录最大规格？

记录到 1W 条日志时，会删除最初的 1000 条。

71 应用自定义 FAQ

71.1 导入自定义应用的规格？

最大规格是 500 条自定义应用，如果导出超过 500 条的文件，则只有导进 500 条成功。

71.2 自定义应用可以用任意的端口号吗？

尽量不要选择已经被使用的端口。

71.3 自定义应用选择规则都必须填写吗？

不是，只需要在目标端口、IP、域名或 URL 任选一个填写即可。

71.4 会话监控里用户和应用没有被识别？

首先用户没有识别，那就是用户地址不在识别范围内，更改用户全局配置里识别范围后，清一下会话，再匹配自定义应用流量过设备。

72 中英文切换 FAQ

72.1 为什么切换成英文版系统日志和操作日志会显示中文日志？

切换成英文版后系统日志和操作日志显示的中文日志是在中文版本操作的，对应的，如果是在英文版的操作后，切换成中文版本，日志也会有英文显示。

72.2 切换成英文版的设备控件显示中文？

设备控件显示中文和操作系统语言有关，操作系统为英文版，浏览器显示设备控件即是英文。

72.3 切换中英文版本会导致配置丢失吗？

不会，保存的配置不受切换版本影响。

73 用户标签 FAQ

73.1 用户标签使用前置条件

- (1) 用户标签是根据网站日志分类进行上报标签，设备需要开启审计策略，需要审计网站类日志
- (2) 用户标签上报前必须配置 imc 服务器的 ip 地址、认证用户名、密码，否则服务器连接认证失败无法上报用户标签。

73.2 标签上报服务器规格

只支持配置一个上报服务器，如果重复配置的话会把之前的 imc 覆盖。

73.3 标签规格

预定义只有 56 个，不支持手动创建自定义 url 分类，其他的 id 号作为预留 url 分类使用。默认所有 URL 分类均参与标签上报通过命令 `url-category (1-1025) user-label enable /disable` 限制哪些标签上报。

73.4 设备记录用户标签规格

用户存储的最大规格为 50x1024，到达规格后老化不活跃用户。

73.5 用户标签使用场景

- (1) 推荐使用于二层场景。
- (2) 用户标签上报跨三层后，设备统计的标签信息 ip 还是终端的 ip，mac 是下联设备的 mac（终端接入的是三层 switch 的情况下，可以配置 snmp 跨三层学习，设备就可以学习到终端 mac（时间需要 30S））。

73.6 用户标签上报类型

每个用户只上报 top3 的用户标签，如果用户标签不足三个，使用 `USER_LABEL_NONE(0)` 填充。

73.7 用户标签存储周期

用户标签信息本地配置文件存储周期为 15 分钟。

73.8 用户标签上报周期

用户标签信息上报 imc 服务器周期为 24 小时。

73.9 日志上报失败的三个条件

- (1) 没有配置 imc 服务器。
- (2) 用户标签文件创建失败。
- (3) 用户标签前台调用的脚本失败。

73.10 日志上报标签错误或者无记录排查

- (1) 查看是不是对应的上报被关闭了。
- (2) 查看保存文件是否是更新了最新的。
- (3) 查看上报文件中的标签是否和保存的一致同时也是更新了最新的。
- (4) debug app audit log 查看是否产生日志。
- (5) 设备开启了审计策略但是没配置 imc 标签上报服务器，默认 24 小时上报一次。

73.11 用户标签启用禁用

User-label enable

User-label disable

73.12 用户标签ID对应关系

分类 ID	中文名称	英文名称
1	广告	ad
2	成人	adult
3	傀儡主机	botnet
4	艺术	art
5	在线音乐	music
6	机动车	automobile
7	BBS站点	BBS
8	键盘记录网站	keyboard-recorder
9	博彩	lottery
10	商业	business
11	计算机与互联网	network
12	犯罪	crime
13	钓鱼网站	fishing
14	毒品	drug
15	教育	education
16	娱乐	entertainment

分类 ID	中文名称	英文名称
17	在线股票交易	transaction
18	证券公司	securities
19	赌博	gambling
20	游戏	game
21	木马病毒	trojan
22	网络资源	network-resources
23	医疗健康	health
24	违反法律	illegal
25	违反道德	immoral
26	求职招聘	recruitment
27	儿童	child
28	法律	law
29	社会生活	society
31	网上交易	trade
32	新闻媒体	news
33	文学	literature
34	在线聊天	chat
35	财经	economics
36	非盈利组织	charity
37	政治	political
38	色情	porn
39	门户网站与搜索引擎	portal-searcher
40	远程代理	proxy
41	房地产	estate
42	参考	reference
43	宗教与信仰	religion
44	科学	science
45	期货	futures
46	银行	bank
47	体育	sports
48	股票	stock
49	基金	fund

分类 ID	中文名称	英文名称
50	外汇	exchange
51	旅游	travel
52	暴力	violence
53	病毒	virus
54	WEB通信	web-im
55	交通住宿预定	hotel
56	白名单	whitelist

74 AD 域单点登录 FAQ

74.1 AD域单点登录仅支持单域

目前不支持多域及子域的情况，在线用户信息未带域名信息。

74.2 关于AD域单点登录启动脚本

单点登录启动脚本，存在被安全类软件提醒的风险。需手动添加至白名单即可。

74.3 关于AD域单点登录数据

用户上报信息已加密，包含用户名、密码。

登录数据此版本不支持防回放。

74.4 AD域单点登录不支持HA同步？

HA 主备单点登录配置支持 HA 同步，但在线用户不支持 HA 同步，如果发生 HA 切换，存在以下两种情形：

(1) 单点登录失败的用户，不需要认证,自动上线。

新的主设备收到用户心跳报文后（默认 30s 发一次心跳报文），用户会重新上线，但是如果上网流量产生在心跳报文之前，则以 IP 作为用户名直接上线。

(2) 单点登录失败的用户，继续匹配后续策略。

新的主设备收到用户心跳报文后（默认 30s 发一次心跳报文），用户会重新上线，但是如果上网流量产生在心跳报文之前，则会继续匹配设备上的后续认证策略，如果没有后续认证策略，则会丢弃在收到下个心跳报文之前的 30s 内的所有报文，后续收到心跳报文后则会重新上线。

74.5 不同用户登录同一台域内测试pc，在线用户只显示一个账号？

在线用户只识别第一次登录的账号，避免频繁出现账号切换，目前设备是基于 IP 来识别用户的，无法实现两个 IP 一样账号不一样的用户同时在线。

75 服务器负载均衡 FAQ

75.1 服务器负载均衡算法

基于源地址散列+权重。

为了保持一致性，同一个源的报文被送到同一个服务器处理，这里需要采取基于源地址 hash 的算法，同时还具有加权随机的算法，最终选择实服务器，即 DNAT 规则。

基于权重。

源 ip 每次都会进行匹配后进行转发。

75.2 权重大小的说明

范围为 1-100。

权值越小，优先级越高。

75.3 探测方式说明

支持 icmp。

通过发送 icmp 数据，检查服务器是否存活。

支持 tcp。

通过发送指定端口的 tcp 数据，检查服务器是否存活。

76 限额策略 FAQ

76.1 限额策略支持流量限额

支持日流量限额。

支持月流量限额。

支持流量提醒功能，达到阈值后，访问 http 后会弹出提醒页面。

76.2 限额策略支持时间限额

支持日时长限额。

支持月时长限额。

支持时长提醒功能，达到阈值后，访问 http 后会弹出提醒页面。

76.3 限额策略惩罚方式

支持惩罚方式为禁止上网。

支持惩罚方式为添加到流控通道。

76.4 惩罚通道的配置

仅支持流控子通道。

需配置一个非常用的服务来作为惩罚的低速通道。

76.5 流量限额提醒功能对https页面访问是否生效？

限额提醒页面对 http 生效，https 页面由于是加密的所以不生效。

76.6 建立多条限额策略,但是同一个用户只能匹配最上面的一条策略,其余策略无法匹配？

限额策略根据五元组从上到下顺序匹配策略，同一个用户只会匹配到一条策略，对于限额实际应用场景来说，时长限额和流量限额是二选一的。

77 无线非经 FAQ

77.1 升级最新非经版本之后，ACG设备上为什么没有无线非经模块

确认设备本身是否有带硬盘，没有硬盘的设备无线非经模块在最新版本上默认不显示。

77.2 开启无线非经功能之后，ACG设备上没有任何审计日志

查看设备上是否有在线认证用户，如果没有在线认证用户（认证用户来源：ACG 设备本身开启认证策略、通过 Radius 监听或者是通过第三方认证服务器发送给 ACG 设备），则不会产生任何审计日志，因为非经日志上报的都是认证用户产生的数据。

77.3 ACG设备上收到了Radius报文，但是并未审计到Radius相关账号信息导致非经日志不产生

最新版本上 Radius 监听功能默认是关闭的，如果需要可在命令行配置模式下执行命令 **user-radius-listen enable** 来开启。

77.4 开启无线非经功能之后，ACG设备本地有审计日志，但是未产生非经日志

(1) 检查无线非经配置策略，场所 AP 是否都已配置；

- (2) 检查测试的应用是否在应用关系对照表中；
- (3) 检查场所 AP 配置是否均已下发（通过命令 **display wxfj-place-cnt** 可确认场所 AP 规格以及下发的场所 AP 数）。

77.5 ACG设备本地产生了非经日志，但是网监平台反馈未收到

- (1) 确认 ACG 设备与网监平台服务器是否能互通；
- (2) 检查数据上报网监平台的账号密码是否都正确（通过命令 **display wireless-cert pbo-entry** 查看）；
- (3) 确认网监平台提供的账号是否有写入权限；
- (4) 排查网络中间是否有配置访问控制阻断策略，阻断其上报数据。

77.6 网监平台反馈上报的上网数据为什么都来自同一个AP

所有数据上报来自同一个 AP，原因是认证数据中没有 APMAC 字段，或者推送过来的 APMAC 字段与 ACG 设备配置的 APMAC 未匹配上，为了数据不丢失，如果认证数据中的 APMAC 字段与 ACG 设备上的未匹配上，ACG 设备上默认进行终端地址范围匹配，终端地址范围默认是 any，所以会出现所有数据都匹配到一个 AP 上进行上报。

77.7 网监平台反馈某些应用日志的账号为真实身份账号，非虚拟身份账号

该类问题主要是由于对接文档要求该字段为必填字段，但使用某些应用不一定会进行登录操作或者登录账号加密无法审计，导致无法获取到虚拟身份账号，所以此类就会填上真实身份账号。

77.8 AP配置导入时，AP导入文件中不能在一个AP上配置多个AP地址范围进行导入

AP 配置导入格式是 csv 格式所致，如果一个 AP 上需要导入多个 AP 地址范围，可以将多个地址对象添加到一个地址对象组中进行导入来实现效果。

78 WEB 页面提示格式化硬盘

78.1 Web页面提示格式化硬盘的条件

- (1) menuboot 下已经格式化的硬盘分区被删除，然后启动支持该功能的版本，打开 WEB 会提示格式化硬盘。
- (2) menuboot 下硬盘分区格式化成 FAT，然后启动支持该功能的版本，打开 WEB 会提示格式化。

78.2 Web页面格式化硬盘后，设备的状态

页面提示格式化，格式完毕后会自动重启，重启后硬盘会自动挂载，WEB 页面不应再有提示格式化硬盘的提示。

78.3 设备启动后，硬盘没有挂载成功？

支持 UI 格式化挂载硬盘的功能，如果硬盘没挂载成功，设备启动后登录页面时会直接返回显示硬盘格式化的操作按钮，可以实现一键格式化挂载。

78.4 设备启动后，硬盘没有识别，UI上不显示硬盘？

UI 上是否显示硬盘是依赖于数据库能否正常连接上，连接不上不会显示，如果数据库创建失败，则会导致硬盘无法显示，处理方法如下：

recover database 重新创建数据库或格式化硬盘即可恢复正常，出现此现象一般是由于两个版本的数据库差异太大导致数据库创建失败，如果升级前后的两个版本差异太大，请升级版本后清库重启。

79 接口及其他 FAQ

79.1 使用40GE的1分4线缆，ACG1000-X1的8个10GE口接上后，接口识别ERROR，最后两个10GE口不UP？

硬件只支持 5 米以下的线缆，如果测试发现接口不 UP，请更换小于 5 米的线缆进行测试。

79.2 接口从地址是否能配置为相同网段？

接口从地址能配置为相同网段的不同 IP，不会发生冲突，这是业内的标准实现。

79.3 设备编码格式是什么？

UTF-8 编码格式，是变长的编码格式，具体如下：

占 2 个字节的：带有附加符号的拉丁文、希腊文、西里尔字母、亚美尼亚语、希伯来文、阿拉伯文、叙利亚文及它拿字母则需要二个字节编码

占 3 个字节的：基本等同于 GBK，含 21000 多个汉字

占 4 个字节的：中日韩超大字符集里面的汉字，有 5 万多个

一个 UTF-88 数字占 1 个字节

一个 UTF-8 英文字母占 1 个字节

即少数是汉字每个占用 3 个字节，多数占用 4 个字节。