UNIS ACG1000 系列应用控制网关

用户 FAQ

目 录

1 部署方式 FAQ

设备应部署在哪里？

设备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。由此来说设备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高要求也可放置设备。但要注意，所有设备应放在区域与区域相接处。

设备部署方式有哪些？

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

什么是路由模式？

当设备位于内部网络和外部网络之间时，需要将设备与内部网络、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，路由模式设备连接两个不同的子网。

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，路由模式设备可以完成 ACL 包过滤、NAT 转换等功能。

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，查看设备安全策略，在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** 命令查看设备安全策略。

什么是透明模式？

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

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。

透明模式的工作原理？

在透明模式下，设备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，设备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。

透明模式的实用性在哪里？

透明模式设备一般使用在原网络拓扑在已经完善的情况下增添设备。配置透明模式设备，设备相当于二层设备。可以将设备的多个接口连接到相同子网。可以在不更改其它设备的路由网关对网络进行保护。减少工作量。

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。旁路模式设备将通过的流量进行监听、审计等作用。

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设备即可。

查看设备日志信息为空时怎么处理？

查看旁路模式设备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** 命令于查看设备的部署策略。

部署设备有什么好处？

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

为什么设备配置正确但是数据无法通过？

设备默认存在一条全拒绝的控制策略，使用设备时应先注意安全策略是否匹配。

接口在修改地址模式为pppoe，由于达到规格下发失败时会清掉原有的静态ip或dhcp配置？

是的，由于在修改下发时需要先清掉接口地址模式的配置然后在下发配置，因此导致原有配置会被清掉，点击取消后也没有了，如果需要原有配置的话，需重新配置下。

配置向导支持哪些使用场景？

此功能主要为了实现设备快速部署于网络中，支持网关模式、网桥模式和旁路模式。

2 设备管理 FAQ

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。

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。

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。

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。

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。

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。

USBkey支持哪些厂商？

USBKey 目前仅支持 epass 一个厂商。

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。

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。

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。

修改https的端口后使用https的方式登录界面，再使用http方式登录失败？

该问题主要原因是由于用户会话的加密导致，原因为：

(1) 首次打开一个登录窗口使用 https 方式进行登录，此时会话 ID 的 Secure 属性为 true，登录成功然后点击退出登录，退出登录后此时页面跳出登录页面，此时登录方式依然为 https 方式，在这种情况下会话 ID 的 Secure 属性依然是 true。

(2) 通过浏览器重新打开一个新窗口，采用 http 方式进行登录，由于未关闭当前会话，所以即使换一个新窗口会话 ID 依然是加密状态，导致加密 session 后台无法识别，所以认证失败。

由于用户登录验证是通过会话 ID，验证码也是通过 session 机制进行的校验，所以造成登录失败。

手动升级相同的特征库日志和自动升级相同特征库日志记录不一致？

特征库的版本号有固定规范不能随意修改添加，但考虑一些特殊局点，需要特殊的特征库，故提供的特征库版本号一致。这种特殊的特征库都采用手动升级的方式，所以手动升级不检测版本号，以手动导入的为准。

NTP时间设定是否支持IPv6服务器地址的时间同步功能？

不支持，目前仅支持 IPv4 服务器。

同一浏览器使用http和https两种方式打开管理页面进行配置，http页面无法登录？

是的，因为安全红线要求，在使用 HTTPS 访问时将浏览器的会话 COOKIE 设置了 Secure 属性，若此时更换访问方式为 HTTP，由于还是同一个会话，COOKIE 是不变化的,同时 Secure 属性仅支持 HTTPS 访问的设置，HTTP 访问无法读取已设置 Secure 的 COOKIE,从而导致登录失败。

处理方法：

(1) 清空浏览器缓存后，刷新页面或关闭浏览器重新打开；

(2) 使用其它浏览器访问。

使用同一主机下登录了一个管理员时，再打开一个管理页面输入另一个管理员密码使之超过最大登录尝试次数，原先正常登录的管理员也会被限制？

是的，管理员登录失败阻断是基于 IP 的，因此原来的管理员也是会被限制的，需要等超过阻断的时间后才能正常登录。

设置多个管理员，同时登录两个管理员时，若退出其中一个，另一个也会退出？

是的，此情况只有在使用同一浏览器登录同一设备时存在，若使用两个不同的浏览器或登录不同的管理设备，在其中一个点击退出时，另一个是不会退出的，因为同一浏览器登录同一设备是使用同一个会话 id 标记的，因此会存在此现象。

管理设定中的页面超时时间提交后不能立即生效，需要清理浏览器缓存才能生效？

是的，使用管理员登录设备，然后修改管理设定中的页面超时时间，提交后未立即生效，管理员没有即时退出，需要清理浏览器缓存才能生效。

设备开启实时保存后使用限制？

设备在开启实时保存后，每次进行配置的时候都会执行配置保存，非常消耗设备资源，因此不建议开启，由于开启后频繁快速操作或者配合 HA 使用时可能存在以下现象：

(1) SNMP 用户同步过程中，连续生成 2 次录入用户任务，第一次的用户录入大概率无法同步到备设备；

(2) IPv4 控制策略引用一条空的 url 对象，然后在 url 对象页面添加内容，概率出现引用关系消失；

(3) 在自动保存配置的过程中，同时删除多个用户，提示信息有误等问题。

这些问题原因都是因为开启了实时保存，设备在执行保存的操作同时又对设备做修改导致的问题。规避手段：如果开启了实时保存，需要在每次执行完配置后等待 1-2 分钟，设备完全保存好配置后在进行相关的操作。

3 IPv4 审计策略 FAQ

如何查看当前的审计策略？

可以使用命令 **display running audit poliy** 查看当前的审计策略。

IPv4审计策略匹配说明

IPv4 审计策略的匹配是从上向下匹配，审计策略里面的源目接口和源目地址都是双向匹配。

审计日志可以存储多少条？

当日志占用空间超过磁盘容量的 90%时就会删除日志，每半小时检查一次，当超过 90%时就会执行删除，未超过 90%时则不进行删除，每次删除最早 1 天的日志，同时对于邮件、邮件附件、网盘文件这种留存的原始文件进行文件个数限制，每天限制最多 10 万个（邮件、邮件附件、网盘存储的文件个数共用同一个 10 万的规格），对于日志没有条数限制，即当此类日志超过 10 万时还会记录相关日志信息，但是无法下载原始文件。

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。

为什么审计不报日志？

(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**。

为什么访问网站未记录网站访问日志？

(1) 检查审计策略是否正确；
(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。

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。

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？

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。

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。

即时通讯审计有哪些限制？

QQ 概率性审计不到退出，偶尔会出现退出跟登录和收发消息是同一条连接，获取不到结束退出的特征，此外有时登录 QQ 也会概率性审计不到登录日志。

微信审计不到退出、收发消息、语音视频，加密应用无法获取到这些行为特征。

阿里旺旺审计不到退出和收发消息，加密应用无法获取到这两种行为特征

社区日志中没有百度贴吧的日志？

百度贴吧需要开启 https 解密才能够进行审计，https 对象中需要包含 BBS 站点;对于百度贴吧应用的网页浏览日志是放在其它应用日志里面的，只有登录和发表时审计日志才会记录到社区日志，而且登录只能审计用账号密码登录的情况，使用手机验证码登录的方式数据单独加密无法进行审计，发布日志由于百度贴吧使用了新的加密方式，目前只能审计到内容，不支持审计账号。

审计日志内容显示会包含部分格式字符？

审计内容的获取是会把部分格式的内容也审计下来，涉及的日志种类很多，由于基本没影响，改动又较大。下个大版本考虑统一做优化。

审计日志导出后打开term_supplier和term_platform两列内容为空？

这两老字段现在没有实际用途，为了保证版本升级数据库兼容性所以保留下来（避免版本升级要清库导致日志丢失），UI 做了屏蔽不会显示。

邮件日志外发时附件个数最多发送5个？

邮件日志外发时，附件个数规格限制为 5 个，最多发送 5 个附件。

邮件日志外发时日志字段中的file_size=0？

由于设备审计邮件是作为整体来审计的，不判断附件个数和大小，在日志外发时再单个拆分附件并统计大小，比较繁琐，非常耗性能，再加上目前并无附件大小统计显示的需求，所以 file_size 按默认显示为 0。

修改微信认证用户模式之后，终端上下线日志用户名未改变？

终端上下线日志是存在数据库中的，模式切换后只有新产生的终端上下线日志才会更新用户名，在线用户处用户名会改变，因为是从内存中保存的用户信息获取的。

分别用不同操作系统(IOS版和Andriod版）终端使用pc开启的wifi进行无线上网，然后登录QQ客户端，在设备的IM聊天软件日志里都识别为Iphone IOS 版？

操作系统类型是通过 HTTP 中的 UA 字段来识别的，用户第一次上网产生的流量携带了 UA 标识，如果后续流量未产生 UA 标识的情况下，会直接取上一次的 UA 标识的操作系统结果来产生日志，因此操作系统显示只能作为参考，不能保证百分之百正确。

文件传输日志HTTP文件下载支持对哪些格式的审计

目前 HTTP 文件下载支持的文件格式后缀如下：

.apk,mpeg,mpg,wma,wav,mp3,aac,compressed,zip,.rar,.gz,.bz2,.tgz,.tbz,.arj,.lzh,.tar,.ace,.uue,.jar,.iso,.7z,.bin,.zip,.txt,.hdr,.doc,.xls,.xlsx,.pacp,.pacpng,.cap,.img,.xz,.exe,.cmd,.bat,.msi,.dmg,.dll,.rpm,.ptada,.gpg,.pdf,.ps,.info,.cat,.cfg,.lss,.msg。

IM聊天软件日志中QQ客户端的收发消息显示为登录？

由于目前 QQ 最新版本收发消息和登录在同一条流中，无法进行阻断，所以将收发消息合并到登录行为中了。

Web mail邮件附件为txt文件的审计，日志页面显示的正确的名称及txt后缀，但下载下来后文件后缀怎么是.tar的压缩文件？

由于目前大部分浏览器对于.txt 格式的文件会自动打开查看而不能进行下载，而且查看的时候浏览器默认使用 utf-8 格式的编码打开，从而导致出现非 utf-8 编码的.txt 文件在浏览器直接打开查看时显示乱码，无法查看审计到的.txt 附件内容，为规避浏览器此问题，目前设备自动对 txt 文件压缩为.tar 格式，这样就能够正常下载到本地解压缩查看了，而页面还是正常显示真实的文件名称及后缀，只是下载时把.txt 文件压缩到.tar 文件来进行下载。

审计日志显示有6000多万条，而页面只能显示出86条，其余都是空白，而导出只有64条且提示信息中不显示导出日志的截止时间？

目前日志总条数的统计是通过计算一天内最大和最小 ID 值的差值来计算的，目的是为了减少统计时间（如果查询真实的日志数量，当日志量很大时查询会很慢，会导致很长时间显示不出总条数和相关的日志展示，很影响用户体验），而页面显示的是数据库中真实存在的数据条目，如果往前修改系统时间就会造成两次写入数据库的 ID 值不是连续的（修改为当日时间和往后修改时间是没有影响的），从而出现计算的日志数量与实际日志数量不一致，出现后面没有数据而显示空白的情况；导出只有 64 条是因为前面 64 条日志是第一次入库时的数据，其 ID 值是连续递增的，由于日志每次导出支持 10w 条是根据 ID 值来进行规格限制的，从而导致后面的 22 条日志未导出（后面日志的 ID 值为 6000 多万，远远大于了 10w），如果想导出后面的 22 条日志，可通过查看页面记录的日志时间，选择时间范围导出即可，由于规格限制是 10w，通过 ID 去取第 10w 条日志是不存在的，由于取不到日志中的时间信息，也就导致显示不出截止时间。

IPv4审计策略为什么没有记录日志，什么情况下才会记录审计日志

审计策略匹配优先级从上至下进行匹配，支持配置多条，不进行去重校验；

由于控制和审计功能独立，不是识别出应用就记录日志的，需要审计到相关应用的账号或内容才会记录审计日志，由于有些是加密传输的，设备无法审计到相关内容，因此测试时需要配合解密的功能。

- HTTP 类审计

(1) 网站访问

匹配条件：

a. HTTP 协议解码模块正确解析获取到 host 字段。

b. URL 库中正确对该 host 进行 URL 分类处理。

c. 审计模块正确审计到网页标题。

注意项：

不开启 https 解密，默认对内置的 https 网页进行审计（https audit predefine），网页标题从内置的网站与标题的对应文件中获取。可以通过命令配置 https audit all 对所有 https 网页进行审计，如果访问的域名在设备内置文件列表中没有查到，则截取域名的一部分当做网页标题，例如(www.soso.com，则网页标题显示为 soso）。

(2) 网络社区

匹配条件：

a. 应用识别模块识别到论坛和微博发帖行为；

b. 审计模块根据审计特征正确提取到发帖内容。

对论坛和微博相关应用的发帖行为进行审计，记录日志到发帖/发微博日志模块。

(3) 网页搜索

匹配条件：

a. 应用识别模块识别到具体的应用搜索行为。

b. 审计模块根据审计特征可以正确提取到搜索关键字内容。

对搜索引擎类、电子商务类的搜索行为进行审计，记录日志到搜索关键字日志模块。

(4) HTTP 外发下载文件

匹配条件：

a. 应用识别模块正确识别到 HTTP 文件传输行为。

b. 审计模块根据审计特征正确提取到传输文件名。

(5) Web 网盘上传下载文件（需开启解密功能）

匹配条件：

a. 通过特征识别网盘文件上传、下载会话，提取文件名信息。

b. 文件内容先缓存在内存中，整个文件的内容缓存完成后，以文件形式写在硬盘上。

c. 通过点击文件传输审计日志里面的文件名，把设备里的文件下载到本地。

注意项：

网页版网盘上传、下载文件支持百度网盘、360 网盘、网易网盘的审计；附件单个文件大小最大支持 100M（也可能是 99.9M，会有一点点的误差）。

- 邮件类审计

(1) SMTP/POP3/IMAP 邮件收发

匹配条件：

a. 应用识别模块正确识别到收邮件行为(IMAP、POP3)或发邮件行为(SMTP)；

b. 审计模块正确审计到邮件发送者、邮件接收者、邮件主题、邮件内容等相关信息。

如果邮件是加密的需要开启 https 邮件解密才能审计到此类行为的邮件

(2) Webmail 发送接收邮件

匹配条件：

a. 通过特征识别邮件附件上传、下载会话，提取附件名、把附件内容首先缓存在内存中，整个附件的内容缓存完成后，以文件形式写在硬盘上；

b. 通过特征识别邮件发送、接收会话，提取发件人、收件人、抄送人、主题等信息；

c. 留存的附件通过附件名与邮件日志关联。

注意项：

a. Webmail 接收邮件只支持 163、126、QQ 邮箱三个，点击收邮件，且得点开邮件查看内容才会有收邮件的请求，才能审计到；如果要审计附件必须点击附件下载，才能审计到；

b. Webmail 邮件发送接收邮件上传下载附件都会先在文件传输中审计到，再关联到邮件审计日志中里面去；

c. Webmail 邮件附件默认最大支持 100M。

- 即时通讯类审计

匹配条件：

a. 应用识别模块正确识别到 IM 登录行为；

b. 审计模块正确审计到 IM 账号信息。

- 基础协议类审计

基础协议审计主要是对各个高层协议进行审计，5.0 支持 FTP 协议审计。FTP 审计主要审计 FTP 协议传输文件名、账号、ftp 操作命令，记录日志到文件传输日志模块。

匹配条件：

a. 应用识别模块正确识别到 FTP 传输文件行为。

b. FTP 解码模块可以正确解析出传输文件名。

- 娱乐股票类审计

娱乐股票类审计目前必须审计到对应的账号或评论之后才能产生对应的审计日志；

娱乐类审计：支持娱乐类应用的账号、评论审计。比如看视频，听音乐，游戏；

股票类审计：支持股票类软件的账号审计；

娱乐股票类审计支持如下应用测试：QQ 游戏大厅登录、优酷视频登录、9188 彩票（需要解密）、大参考登录。

- 网络应用类审计

网络应用行为审计主要对其它网络应用中能获取到账号的应用行为进行审计，记录日志到其它应用日志模块。

电子商务类登录有审计账号的都会在网络应用类审计中产生其它应用日志。

4 IPV4 控制策略 FAQ

IPv4控制策略匹配说明

IPv4 控制策略匹配是从上向下匹配，源目接口单向匹配，例如报文是从 ge0 入从 ge1 出，此时策略只能匹配到源接口为 ge0，目的接口为 ge1 的控制策略。

IPv4控制策略里子策略配置说明

新建 IPv4 控制策略和子策略后取消，整个 IPv4 控制策略不下发。

当在已存在的 IPv4 控制策略里新建子策略后，点击取消，子策略会一起下发。IPv4 控制策略和里面的子策略是不同的配置页面，在 IPv4 控制策略里新建子策略提交后，子策略的配置就已经下发成功。

HTTP上传关键字检测不支持压缩文件检测？

不支持，压缩文件上传时不是明文的，无法检测到关键字。

关键字过滤不区分大小写字母？

关键字过滤不区分大小写字母，无论配置为大写或小写均可正常检测和过滤。

关键字过滤同一条流只过滤第一个关键字？

关键字过滤同一条流只要检查到第一个符合条件的关键字就会停止匹配。

论坛和邮件附件上传是否支持附件内容过滤？

不支持附件内容过滤，只支持基于附件名过滤。

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。

FTP应用是否支持关键字过滤？

FTP 应用暂不支持关键字过滤。

网页内容关键字过滤存在网页加载不全的情况？

网页内容过滤时，有时关键字在网页中的位置比较靠后，此时检测到关键字后，部分网页内容已经加载成功，所以会出现网页部分加载的情况。

在应用对象自定义应用中添加一个域名为www.baidu.com的应用，并将应用类选择为搜索引擎类，此时在IPv4控制策略中基于WEB搜索引擎关键字过滤时，百度搜索关键字不生效。

WEB 搜索引擎关键字过滤是针对设备预定义应用中已经提取了搜索关键字特征的应用进行过滤操作，虽然百度搜索引擎在预定义搜索引擎中，但是自定义应用中又配置了百度相关的域名，此时应用识别的时候会优先识别自定义应用，从而无法走到预定义百度搜索的识别中去，所以导致百度搜索关键字基于 web 搜索引擎关键字过滤不生效。

邮件控制都支持哪些？

邮件控制只支持 SMTP 客户端发送邮件进行控制，收邮件均不支持控制，网页邮箱等也不支持。

邮件控制中匹配控制顺序是什么？

配置好邮件控制后根据发送 smtp 邮件进行控制，匹配邮件控制顺序为：发件人->收件人->邮件大小->附件个数->邮件主题->邮件内容。

邮件控制中支持匹配几个关键字？

邮件控制中收件人过滤、收件人过滤和标题及内容关键字均只支持选择一个关键字。

邮件控制关键字匹配原则是什么？

关键字匹配规格为发送邮件中的关键字包含配置的自定义关键字才能匹配；反之则不会匹配邮件控制。

虚拟账号规格？

单条控制策略只能引用 1 个关键字对象。

关键字规格？

关键字条目规格 512 和 1024 条，每个关键字对象里可以配置 1024 个关键字。

虚拟账号匹配？

QQ 账号黑白名单关键字控制，关键字匹配为精确匹配。

苹果系统虚拟账号不支持？

苹果系统虚拟账户控制不生效，特征加密问题。

虚拟账号控制依赖条件？

虚拟账号控制依赖应用特征库，特征库不识别时无法控制。

安卓移动端虚拟账号使用限制？

移动端（安卓）测试虚拟账号控制时，需要关闭移动网络。

旁路模式虚拟账号使用限制？

旁路模式 qq 阻断不生效。

虚拟账号日志产生条件？

虚拟账户匹配到白名单，应用控制不产生日志（只有黑名单阻断后才产生日志）。

配置的虚拟账号阻断，应用控制放行 qq登录阻断前后会有一条放行的日志？

QQ 登录识别报文和获取账号报文不在同一个报文中，前一个报文识别为 QQ 登录，未获取到 QQ 账号，命中了应用控制策略报放行日志。后一个报文获取到 QQ 账号，命中了虚拟账号策略，报阻断日志，此情况属于正常现象。

为什么配置终端公告功能，内网用户访问时，未弹公告页面？

终端公告正常弹出需要满足以下条件：

- 策略开启终端公告提醒，接口管理方式必须开启 http。

- 终端访问 http 页面，才会触发弹出公告，目前不支持 https。
- 终端公告提醒前置条件，终端能正常访问公告页面。

为什么内网安卓手机打开浏览器没有弹出终端公告？

安卓手机后台会偷跑 http 流量，所以有些时候，打开浏览器没有弹出公告，这个时候需要保证后台运行的其它软件没有触发 http 流量。

配置的定时推送功能，推送时间已过的情况下，新上线用户还会推送么？

用户若第一次上线（在线用户中没有此用户即为第一次上线），即使定时推送时间已过，也会弹终端公告。

配置的定时推送功能，推送时间已过，为什么没有推送出公告页面？

公告页面的推送基于间隔的是间隔时间推送一次，基于定时的是过了此时间点推送一次，推送过后在下次时间点未过之前就不再推送了，虽然目前已有 UA 过滤，尽量避免非浏览器的推送，但做不到完全过滤掉非浏览器的报文，建议基于时间点的推送如果没有推送出来，可通过注销在线用户再次使用浏览器查看能否正常推送出来，如果能够推送出来那就表示功能正常（注销用户会把其记录的已经推送过的标记清掉）。

为什么配置基于多终端的控制策略，内网多终端用户却没有匹配控制策略？

首先要看在线用户中此用户的终端类型是否识别为多终端，只有识别成多终端的情况下，才会匹配此控制策略。

微信内收发文字消息不产生应用控制日志？

微信中收发文字消息被加密，无法识别此加密行为。

自由门软件无法识别和控制？

自由门软件实现机制比较特殊，提取不到有效的特征，目前暂无法识别和控制。

Ipv4控制策略网络协议动作配置为允许时不发日志？

基础网络协议日志量太大，为了避免大量刷日志，做了特殊处理，只有在阻断的时候才会产生日志，动作为允许时不发日志。

应用控制阻断文件传输，网页中的图片仍然可以下载成功？

HTTP 下载针对网页中的图片不做识别，否则会影响网页浏览，且 HTTP 下载的识别针对特定类型的文件后缀生效：

.bin,.zip,.rar,.gz,.bz2,.tgz,.tbz,.arj,.lzh,.tar,.ace,.uue,.iso,.7z,.txt,.hdr,.doc,.xls,.xlsx,.pcap,.pcapng,.cap,.img,.xz,.csv,.p12,.crt,.data,.exe,.cmd,.bat,.msi,.apk,.dmg,.dll,.jar,.rpm,.ptada,.gpg,.pdf,.ps,.info,.cat,.cfg,.lss,.msg,.odt,.pom,.gem,zip,.mpeg,.mpg,.wma,.wav,.mp3。

QQ发送文件，为什么有时候显示有阻断日志，但是现象却是发送出去了？

QQ 发送文件如果是秒传文件那是无法阻断的（秒传文件指之前曾经传输过的文件，或者是从公众网站上下载的一些安装包），之前传输过的文件或公众网站上的一些安装包，腾讯服务器上已经保留了文件的 MD5 等信息，当再次传输这个文件的时候，腾讯服务器上发现存在相同的 MD5 文件，这个时候 QQ 就采用一种特殊的方式，快速的把这个文件传送到接收端，而 QQ 客户端并没有真实的发送文件，所以就阻止不了，导致看到的现象是对端收到了文件，没有阻断掉。

控制策略引用自定义url匹配说明

(1) 配置自定义 URL，无论 IPv4 策略是否引用，都会对访问的 URL 按照配置的自定义 URL 以类的方式识别。如果 IPv4 策略引用自定义 URL，则对引用的对象进行放行或者阻断。

(2) URL 匹配配置的自定义 URL 是支持模糊匹配的，优先精确匹配，匹配不到再进行模糊匹配。例如策略引用了两个自定义 URL，名称分别为门户网站和测试网站，门户网站包含 URL 为“www.sina.com”，测试网站包含 URL 为“sina.com”，当访问 www.sina.com 时会优先匹配到“www.sina.com”，URL 即属于名称为门户网站的自定义 URL，当访问 sport.sina.com 时，会匹配到“sina.com”，URL 即属于分类为测试网站的自定义 URL。

5 策略分析 FAQ

策略分析功能有什么作用？

当前网络环境的复杂性，网络服务与网络终端的多样性，相应的设备就需要更多、更复杂的控制策略。这些控制策略经过一段时间的积累，往往会造成老策略不敢删，新策略不断增加，单台设备会积累成千上万的策略，极大降低设备性能和用户体验。

从策略分析的角度，一键分析当前的冲突、冗余、隐藏、合并、过期和空策略，一定程度上解决防火墙管理的难题，使每一条策略都直观可视，让设备更易于使用、便于维护管理。

策略分析能检测哪几种策略情况？

冲突策略：不区分匹配的前后顺序，若策略 A 和策略 B 存在数据流交集（非包含和被包含关系），且 AB 策略的行为不同，则 A 和 B 互为冲突策略。

冗余策略：根据匹配的前后顺序（先匹配 A 策略再匹配 B 策略），如果 A 策略匹配的所有数据流会被 B 策略包含在里面，删除 A 策略不会对其余策略产生影响，如果 AB 策略行为相同，那么 A 策略会被计算为冗余策略。

隐藏策略：根据匹配的前后顺序（先匹配 A 策略再匹配 B 策略），如果 B 策略匹配的所有数据流会被 A 策略包含在里面，如果 AB 策略行为相同，那么 B 策略会被计算为隐藏策略。

可合并策略：不区分匹配的前后顺序，策略内元组信息只有一项不同（且可合并）的情况下，则认为是可以合并的策略。

空策略：当策略中匹配的任何一个对象为空时，那么该策略会被计算为空策略。

过期策略：发现当前策略中，匹配的时间范围已经不会再次出现的策略。

策略宽松度如何定义的？

极宽松、较宽松、正常、准确以引用的源地址、目的地址中包含的实际 IP 地址数目换算得到，大于 65535 个 IP 为极宽松，256-65535 为较宽松，32-256 为中正常，小于 32 为准确。

为什么策略引用过期用户，被分析成空策略而不是过期策略？

因为过期用户和配置为空的用户组处理方式一样，无法区分，因此被分析为空策略，目前过期策略只支持时间过期。

6 IPV6 控制策略 FAQ

IPV6控制策略以及子策略都可以配置多条重复策略？

IPV6 控制策略以及子策略未对重复策略进行去重处理，由于应用对象有变化，为了兼容之前老版本配置，所以此处未进行去重处理；且 IPV6 控制策略匹配也是由上至下进行匹配，匹配到策略之后不会再往下继续匹配，所以配置多条重复策略，只有前面第一条生效，后面的都将匹配不到，不影响功能使用。

配置了IPV6控制策略，用户过设备访问外网IPV6资源没有匹配IPV6控制策略？

确认设备上是否启用 ipv6 enable 功能，此项通过命令行配置查看，其次用户识别范围是否包含 IPV6 地址（此项可以将识别范围修改为 any，或者将识别方式修改为启发模式）。

7 流控 FAQ

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。

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。

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。

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。

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际的带宽一致，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。

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。

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。

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。

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。

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。

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。

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**。

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。

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%。

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。

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≥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≥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。

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。

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。

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。

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。

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。

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。

哪些报文不受QOS限制？

本地报文、非 IP 报文，另外桥接口报文只受物理口 QOS 策略限制不受桥口 QOS 策略限制。

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。

限制通道和普通通道的匹配优先级是什么？

同一个接口既配置普通通道又配置限制通道，只会匹配限制通道，命中限制通道后不会继续匹配。在外网口和内网口同时配置限制通道和普通通道，先匹配流量流入接口的策略，再匹配流量流出接口的策略。

流量经过限制通道和普通通道时统计的流量大小不一致？

为了提升 QOS 限制通道的处理性能，目前流量统计粒度比 QOS 通道的粗，流量统计存在 5%左右的误差。

限制通道、惩罚通道、普通通道的规格是多大？

限制通道、惩罚通道、普通通道共用总规格 256。

限制通道不依赖于线路？

新增的限制通道和惩罚通道不需要绑定线路，与 QOS 线路并列显示，因此限制通道与线路和其它限制通道可以配置同一接口。

惩罚通道的用途是什么？

惩罚通道提供给限额策略引用，可以实现有条件的进入带宽限速，单独配置没有任何影响，只在限额策略引用之后生效。没有启用禁用选项。

惩罚通道支持升级配置兼容吗？

支持，低版本是基于 QOS 通道来实现惩罚通道功能的，升级到支持惩罚通道功能的版本时，当设备重启后会自动删掉被限额策略引用的 QOS 通道，然后自动创建同名的惩罚通道，保证配置兼容。

两个方向的UDP单向流都命中惩罚通道的出方向带宽限制？

一条流包正反两个方向，对于 TCP 流，设备根据流量发起方确定为正向流，匹配出方向带宽限制，五元组相同的另一个方向的反向流则匹配入方向带宽限制，对于 UDP 流由于无法区分正反向，会将流量进入设备的那一个方向确定为正向流，匹配出方向带宽限制，五元组相同的然后另一个方向

的流确定为反向流匹配入方向带宽限制。综上，如果使用测试仪模拟 UDP 流量，两个方向的流如果五元组不一样，则均为 UDP 单向流，会同时命中惩罚通道出方向带宽限制。

8 首页 FAQ

为什么首页行为管理中审计日志没有统计计数展示？

该功能依赖硬盘，如果没有硬盘的设备，数据不做统计，如果有硬盘的设备，统计全部是以当天的维度，显示当天总的审计日志条数及具体每个审计模块的日志条数。

为什么首页行为管理中流量分析没有分析展示？

该功能需要配合流控策略使用，支持 2 条线路质量分析，统计线路下行带宽数据来分析整体线路质量。

首页的在线用户统计哪些用户？

首页的在线用户中只统计认证用户和匿名用户，点击在线用户可跳转到在线用户页面。

首页的系统日志为什么和系统日志页面的记录不一样？

首页的系统日志只报级别是警告及以上的最近 20 条日志。

首页的审计日志是统计所有的日志么？

首页的审计日志统计各日志当天的记录，并可以点击每一类日志进行详细日志查看。

首页的阻断用户数都统计哪些用户及行为？

策略违规展示的是应用控制日志中阻断用户。

共享终端违规展示的是共享接入监控中的阻断用户（阻断和限速）。

限额违规展示的是限额策略中限额用户统计中阻断用户（禁止上网和限速）。

首页的流量分析评分标准是什么？

流量分析显示并统计当前流控策略的线路，默认统计前两条流控策略的线路；线路值只统计线路下行带宽，每 10s 刷新一次。

具体的评分标准是：

- 单条线路

线路优=80：使用带宽占比低于 50%；

线路良=60：使用带宽占比高于 50%，低于 60%；

线路中=50；使用带宽占比高于 60%，低于 80%；

线路差=40；使用带宽占比高于 80%。

- 整体评估

整体线路评分值为：线路 1 评分值*（线路 1 带宽限速值/（线路 1 带宽限速值+线路 2 带宽限速值））+线路 2 评分值*（线路 2 带宽限速值/线路 1 带宽限速值+线路 2 带宽限速值）

整体线路评级标准：

优：整体线路评分值大于等于 80；

良：整体线路评分值大于等于 60，小于 80；

中：整体线路评分值大于等于 50，小于 60；

差：整体线路评分值小于 50。

举例说明：

- 单条线路：

线路名	线路带宽	实时流量
123	30M/40M	29.8 (Mb/s)/31.1 (Mb/s)

31.1/40*100%=77.75%,根据评分标准，此线路质量为中。评分标准如下：

线路优=80：使用带宽占比低于 50%。

线路良=60：使用带宽占比高于 50%，低于 60%

线路中=50；使用带宽占比高于 60%，低于 80%

线路差=40；使用带宽占比高于 80%

- 两条线路：

线路名	线路带宽	实时流量
123	30M/40M	29.8 (Mb/s)/31.1 (Mb/s)
sdf	30M/40M	29.8 (Mb/s)/28.0 (Mb/s)

线路 123：31.1/40*100%=77.75%,根据评分标准，此线路质量为中，则线路 123 的评分值为：50。

线路 sdf：28.0/40*100%=70%,根据评分标准，此线路质量为中，则线路 sdf 的评分值为：50。

评分标准如下：

线路优=80：使用带宽占比低于 50%。

线路良=60：使用带宽占比高于 50%，低于 60%

线路中=50；使用带宽占比高于 60%，低于 80%

线路差=40；使用带宽占比高于 80%

整体线路评估：

线路 1 评分值*（线路 1 带宽限速值/（线路 1 带宽限速值+线路 2 带宽限速值））+线路 2 评分值*（线路 2 带宽限速值/线路 1 带宽限速值+线路 2 带宽限速值）=50*(40/(40+40))+ 50*(40/(40+40))=50, 根据评分标准，此整体线路质量为中。评分标准如下：

优：大于等于 80

良：大于等于 60，小于 80

中：大于等于 50，小于 60

差：小于 50

9 监控统计 FAQ

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。

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。

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。

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。

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 接的状态信息。

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。

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。

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。

设备健康统计采集规则

(1) 最近 1 小时，1 分钟采集一次。

(2) 最近 4 小时，5 分种采集一次。

(3) 最近 1 天，10 分钟采集一次。

(4) 最近 1 周，1 小时采集一次。

为什么在同一时刻，监控统计中的会话统计与设备健康统计中的会话统计存在误差？

监控统计中会话统计与设备健康统计中会话统计，同一时刻数据存在误差，是由于两个功能采集方式不一致导致，会话监控采集周期是 1 秒一次，而设备健康统计中最小采集周期是 1 分钟一次

支持时间段查询，为什么有时点击页面没有反应？

支持选择时间段查询，必须点击到数据点才可以，如下图：

(1) 最近 1 小时，不支持选择时间查询；

(2) 近 4 小时->1 小时，只有后三个小时支持选择时间查询，最近一小时不支持，需要切换统计时间查询；

(3) 最近 1 天->4 小时->1 小时，只有后 20 个小时支持选择时间查询，最近 4 小时不支持，需要切换统计时间查询；

(4) 最近 1 周->1 天->4 小时->1 小时，只有后 6 天支持选择时间查询，最近 1 天不支持，需要切换统计时间查询。

导出的功能的数据范围是什么？

导出功能只能导出最近一周的数据，也可以通过命令（**export health statistic info tftp**）导出

导出数据中内存的三列都是什么？

导出数据中内存会展示三列：全部内存、控制内存、数据内存。

如何开启/关闭内存页面的数据面内存和控制面内存展示？

页面默认只展示全部内存数据，可以通过命令（**health memory detail info enable|disable**）打开及关闭展示控制内存和数据内存。

所有页面都存在定时刷新功能吗？

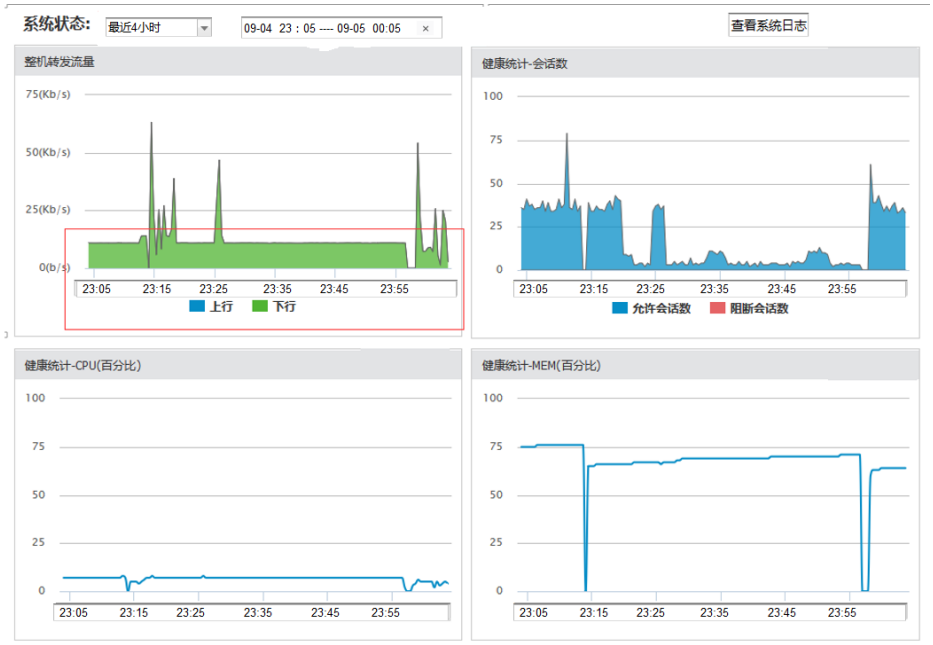
只有统计时间为最近 1 小时，才有定时刷新功能，周期为 1 分钟。

修改系统时间后，页面数据如何展示？

设备运行过程中，设备修改了系统时间，统计数据展示不会根据时间来丢弃原有数据，只有掉电重启后，才会根据修改后时间来展示数据。

查看的时间区间不在同一天，页面如何显示？

如果查看的时间区间不在同一天，以最近 4 小时（时间范围 2018-09-04 22:05—2018-09-05 02:05）为例：在最近 4 小时页面，点击其中“23:05—00:05”区间，页面显示时间范围图标为：



设备健康统计优化页面统计的数据是瞬时值还是平均值？

(1) 流量统计：采集的是平均值。

(2) 会话数：允许和阻断，采集的是瞬时值。

(3) CPU 信息：加权平均值，假如采集点是 1 分钟一个，那 1 分钟收集 12 个瞬时值，然后将这 12 个值进行平均计算。

(4) 内存信息：采集的是瞬时值。

(5) 会话信息：当前会话数和新建会话数，采集的是瞬时值。

设备健康统计的数据存在哪？多久存一次？什么情况下会丢？异常情况下的自我保护功能怎么样？ 例如CPU繁忙、内存繁忙、异常断电、进程挂死等。

(1) 目前统计信息存储在/mnt/目录下，设备启动之后，1 分钟保存一下临时数据，15 分钟保存到/mnt/目录下。

(2) 正常重启前（比如执行 reboot），会将临时数据保存到/mnt 目录下；异常情况，比如断掉或者 nmi，无法及时将临时数据拷贝到/mnt 下。

(3) cpu 繁忙会影响数据的记录（定时器得不到调度），只要 dplane 进程不挂死，就可以正常收集数据，如果 dplane 控制核挂死，无法记录数据。

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。

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。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。

会话监控页面上用户/用户组列有些显示具体的用户及用户组，有些显示为空？

如果该会话不在用户识别范围中，则无法获取到对应的用户及用户组，所以会话监控统计页面上用户及用户组显示为空。

HA备机设备会话监控中用户和用户组不显示？

因为 HA 主备环境下不同步匿名用户，备机上有没有相关流量识别匿名用户，所以备机上没有此相关用户，从而不显示。

会话监控，某些ip提取不到用户名和组？

用户和组显示为空的几个可能原因：

1、匿名用户超过最大限制（在线用户规格）

超过限制之后，设备会踢掉一些在线用户（最早的上线的那个），此时会话仍然存在。

2、会话刚创建还未进行识别

这种情况下的隔一小会儿就会正常识别。

3、会话老化

会话老化的也会主动将用户信息清除。

4、用户注销或老化

5、用户不活跃超过 20 分钟，系统内部有一个定时器，超过 20 分钟不活跃的用户也会被清除。

10 用户信息中心 FAQ

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。

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。

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。

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。

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；

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它。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，只是放在其它里统一呈现。

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 为其它类的日志数，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。

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。

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。

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。

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。

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。

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。

11 安全分析 FAQ

安全事件分析包含了哪些功能日志？

安全事件分析包含入侵防御检测日志、WEB 防护日志、防暴力破解日志、网络层攻击日志（只统计扫描攻击防护日志）。

安全事件分析中的级别，如何定义的？

在安全事件分析中呈现的级别是根据该攻击源中产生的最高级别攻击日志展示的。

资产安全分析包含了哪些功能日志？

资产安全分析包含入侵防御检测日志、WEB 防护日志、弱密码防护日志、防暴力破解日志、网络层攻击日志（只统计扫描攻击防护日志）、病毒防护日志、非法外联日志、行为模型（DNS 隧道）日志。

各种类型日志，使用资产 IP 做检索，不同的安全日志检索的源和目的不同，说明如下：

- 入侵防御日志：基于目的地址统计；
- WAF 日志：基于目的地址统计；
- 弱密码防护：基于目的地址统计；

- 防暴力破解日志：基于目的地址统计；
- 网络层攻击（扫描攻击防护日志）：基于目的地址统计；
- 病毒防护日志：基于源地址统计；
- 非法外联日志：基于源地址统计；
- 行为模型（DNS 隧道）：基于源地址统计。

资产安全分析中级别如何定义的？

风险计算算法，通过计算威胁事件条数来确定风险级别（1-100 为低风险，101-200 为中风险，201 以上为高风险）。

12 策略路由 FAQ

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。

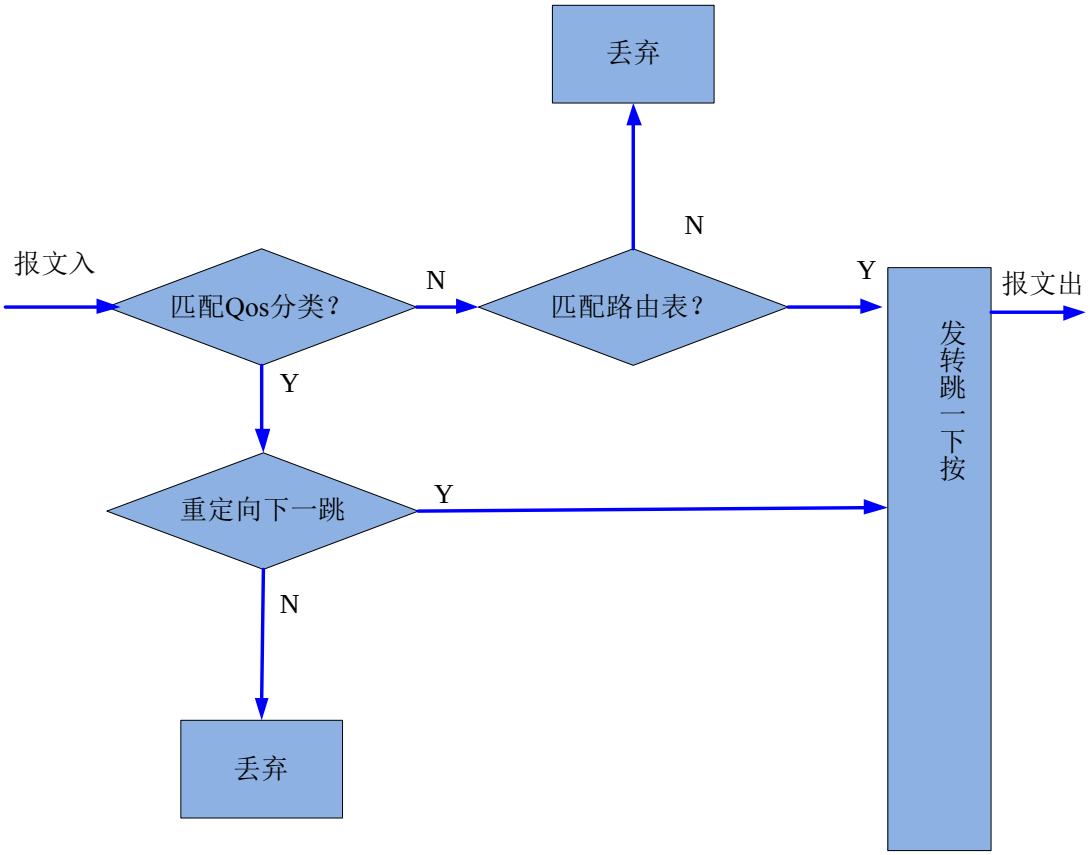
同一条策略路由最多支持几个下一跳？同时配置多个下一跳的情况下，如何转发报文？

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。

策略路由转发流程图

图1 策略路由转发流程图



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。

13 ISP 路由 FAQ

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。

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。

ISP路由是怎样工作的？

用户在 ISP 路由配置页面新建策略，可以引用 ISP 信息预定义的运营商网段表，使相应 ISP 路由生效，同时支持在 ISP 信息页面自定义创建新的 ISP 对象，添加对应的目的地址网段，然后在 ISP 路由页面创建策略来引用以使其生效。

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。

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。

14 IPsec VPN FAQ

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.
*************************************************
```

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.
*************************************************
```

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。

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。

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**。

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**。

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。

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。

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。

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。

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。

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。

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。

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。

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
```

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。

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“<>”否则有可能会出现显示报错，但 不影响最终使用，尽量避免。

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。

主链路被引用后还能继续当做其它链路的备链路吗？

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它链路引用。

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。

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。

链路断开是监控哪个阶段？

主备链路监控的是 IPSEC SA 的状态。

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。

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

15 IPv6 FAQ

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。

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。

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。

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。

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。

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，目的节点通过在本地链路上发送 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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

什么中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。

16 VRF FAQ

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。

设备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)。

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。设备的 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。

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。

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。

VRF模块设计背景？

VRF 模块属于设备的功能模块，实现虚拟路由转发功能。

VRF接口支持哪些功能？

绑定了 VRF 的接口，仅支持 NAT 和静态路由功能，不支持其它功能，例如 IPSec VPN、动态路由等。

VRF接口ping不通？

接口加入 VRF 后，ping 本机 VRF 中的接口地址 ping 不通，对端直连设备也无法 ping 通本端 VRF 接口的地址。

17 动态路由 FAQ

RIP支持v1和v2功能吗？

RIP 支持 v1 和 v2 两个版本。

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。

OSPF是否支持pppoe接口？

Ospf 不支持 pppoe 接口。

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。

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。

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。

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。

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：两端的了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 的数据库是脱节有问题的（在我的 Router LSA 中，我认为你是个广播邻居；而在你的 Router LSA 中认为我应该是个 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。

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。

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）。

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。

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。

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。

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。

18 HA FAQ

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。

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。

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。

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。

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。

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。

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。

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。

心跳报文

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

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。

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。

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。

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。

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。

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。

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。

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。

19 Bypass FAQ

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。

Bypass接口使用在哪种网络场景中？

使用在二层网络场景。

Bypass功能默认开启吗？

Bypass 功能默认开启。

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。

系统运行过程断电是否会触发Bypass？

异常断电会触发 Bypass。

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。

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。

20 APP 缓存 FAQ

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。

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。

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。

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。

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。

APP动态缓存的规格？

APP 动态缓存最多可以写 8 个域名。

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）。

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。

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。

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。

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。

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。

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。

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。

APP动态缓存设备http服务端口必须为80，不支持端口漂移？

是的，目前 APP 缓存 302 重定向设备服务端口必须为 80，不支持端口漂移，如果管理端口被修改后配置的动态缓存的应用将无法下载。

21 会话限制 FAQ

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。

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。

		地址对象	会话限制	每秒新建限制	操作
1		技术支持组	100	10	
2		any	200	10	

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。

	IP地址	连接数	会话限制	每秒新建	每秒新建限制	限制阻断统计	地址对象
1	0.0.0.0	1	200	0	10	0	any
2	192.168.2.1	1	100	0	10	0	技术支持组
3	192.168.2.4	1	100	0	10	0	技术支持组
4	192.168.2.23	2	100	0	10	0	技术支持组
5	192.168.2.129	11	100	0	10	0	技术支持组
6	192.168.2.130	2	100	0	10	0	技术支持组
7	192.168.2.148	1	100	0	10	0	技术支持组
8	192.168.2.185	1	100	0	10	0	技术支持组
9	172.168.100.1	1	200	0	10	0	any

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？

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。

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。

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。

22 DNS 代理 FAQ

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

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。

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。

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。

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。

DNS接口类型改变后dns无法解析

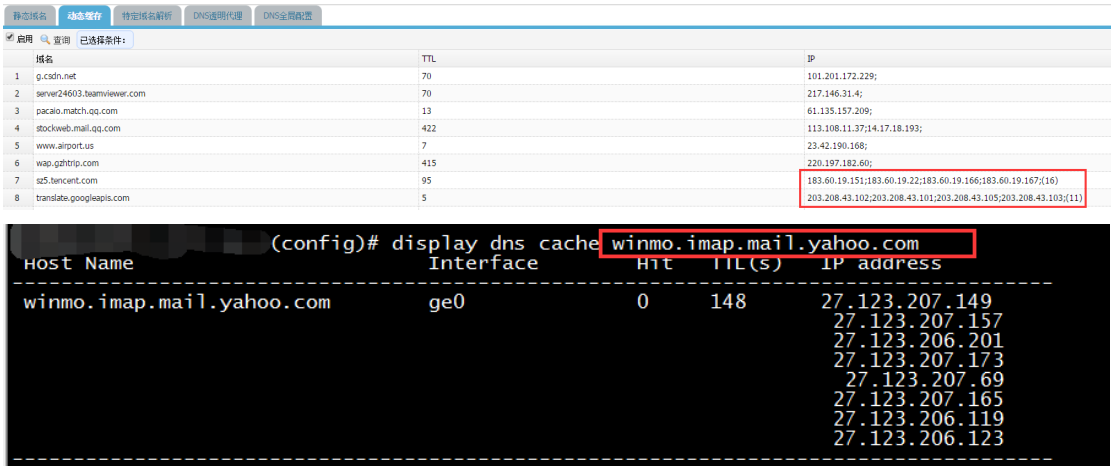
接口类型改变后必须去手动修改 DNS 链路的配置，否则会造成业务不通。

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。

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

启用 查询 已选择条件：

	域名	TTL	IP
1	g.csdn.net	70	101.201.172.229;
2	server24603.teamviewer.com	70	217.146.31.4;
3	pacaio.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	sz5.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)

```
(config)# display dns cache winmo.imap.mail.yahoo.com
 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
-------------------------------------------------------------------------------
```

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。

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。

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。

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。

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

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。

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。

为什么进行包含域名的策略控制会放行一段时候后才可匹配策略？

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间差。

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。

dns透明代理的会话是不是查询不到？

是的，由于 dns 报文被重新组装发送而不是基于会话转发的，所以查询不到。

23 入侵防御 FAQ

为什么配置入侵防御后无法生效？

是否没有更新最新入侵防御特征库。

规则中包含的签名集是否包括要检测的签名

规则中包含的签名集需要包含要检测的签名。

什么时候需要开启入侵防御相关配置

防止外部攻击防御，开启该功能以预防。

24 病毒防护 FAQ

病毒防护支持哪些压缩格式的文件？

目前支持对 zip、gz、bz2 等压缩文件进行扫描。

FTP协议病毒文件可正常检测并报，但病毒文件仍然下载成功？

FTP 客户端软件下载部分文件存在概率出现断点续传的情况，被阻断的报文会另起会话进行传输。

IMAP协议传输病毒文件概率性出现病毒文件下载成功？

某些情况下 IMAP 协议传输会出现大量报文乱序的情况，目前设备默认规格是支持 20 个乱序报文重组，已新增命令 application tcprsm level [20-80]可配置支持重组乱序报文个数是 20-80 个。

FTP传输使用ASCII或文本传输病毒文件无法检测？

只支持二进制方式传输，一般 FTP 客户端默认是自动选择传输方式，优先使用二进制方式。

WebMail邮件上传的部分带病毒附件不能阻断？

WebMail 只支持 126/163 邮箱，且单个附件存在分多个 post 上传的情况，此种情况无法识别。

病毒防护，对于filezilla等这种支持断点续传的ftp无法阻断？

是的，病毒防护功能是通过计算传输文件的 MD5 值和特征库比较来确认是否为病毒文件的，计算 md5 的时候需要文件已经是一个收集完整的文件，而断点续传的话，有可能属于多条流，目前无法组合多条流相关数据来统一计算 md5，从而无法进行阻断。

25 安全防护 FAQ

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。

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。

DNS隧道检测支持什么组网模式？

支持网桥模式、路由模式、旁路模式，其中旁路模式只支持检测，其余模式支持检测和阻断

DNS隧道检测方式的适用场景？

基于异常报文检测方式适用设备部署在 NAT 后场景，所有和基于流量模型检测适用于除 NAT 后之外的场景。

行为模型日志规格？

dns-tunnel 日志一天最多入库 5W 条，超过 5W 条后，覆盖最早的日志。

行为模型缓存规格？

dns-tunnel 缓存规格 5000 条包括所有 dns-tunnel 的流量。规格超了，就走 dns-tunnel 检测流程。

行为模型日志记录？

Dns 隧道动作允许和拒绝都可以记录日志。

行为模型动作为拒绝并加入黑名单后续处理流程？

dns-tunnel 报文匹配阻断并且加入黑名单后，后续的报文再过来直接在黑名单那里就阻断，不会再走 dns 隧道检测流程。

行为模型预置白名单？

预置白名单是指在（网络配置-基础网络-DNS 服务器下配置的 DNS 服务器地址）勾选后不会再走 dns-tunnel 流程。

行为模型自定义白名单规格？

最大支持 64 个自定义 DNS 服务器地址。配置后不会再走 dns-tunnel 流程。

行为模型与全局白名单的关系？

全局白名单开启后不会再走 dns-tunnel 流程。

反向报文触发的dns隧道日志记录？

桥和旁路模式，并且是反向报文触发攻击日志的发送的情况，mac 记为：-。

行为模型日志记录实现说明？

相同源、目的 ip、源端口的 dns-tunnel 流 5 分钟报一条日志，日志发送是没锁的，偶尔可能间隔不完全准确。

行为模型日志行为描述两种情况说明？

记录的是检测到 dns 隧道的原因，有两种情况，一种是满足 dns 请求报文个数超过阈值，记为：

DNS 流量过大，一种是既满足请求报文个数超过阈值又存在异常报文情况，记为：DNS 流量过大且存在异常报文。

26 WEB 防护 FAQ

WEB防护中的CC攻击防护在修改防护范围的时候访问次数会变成默认值

CC 攻击防护的防护范围配置在全站和指定 URL 这两个方式只能选择一种，全站的防护的范围会比较广，所以默认给的阈值比较大，指定 URL，是针对某一个 URL 的访问防护，所以默认阈值比较小，在进行切换的时候，由于全站的访问次数配置的比较大，切换到指定 UR 防护，不进行修改的话会影响指定指定 URL 的防护效果，反之指定 URL 配置的较小，切换到全站如果不进行修改的话会造成误阻断，所以切换方式的话就默认变成了推荐值，防止影响 CC 攻击防护功能的使用效果。

Web防护分析的日志规格？

规格防护支持统计最近 1W 条规则防护日志进行分析，高级防护支持统计最近 5W 条高级防护日志进行分析。

27 统计集 FAQ

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 天的刷新监控是 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。

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。

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。

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。

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%。

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。

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%。

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。

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。

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。

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。

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。

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。

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。

28 地址探测 FAQ

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。

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。

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。

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。

设备配置HA并且关联track，主墙无法切换？

(1) 设备备墙上查看 HA 配置。

(2) 设备备墙上查看 HA 所关联 track 状态是否为 Failed。

(3) 设备备墙查看引用的 track 对象的探测目标是从哪个接口出去的。

(4) 设备备墙在探测目标的接口下配置管理 ip 地址。

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。

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。

29 策略优化 FAQ

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。

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。

30 IMC 联动 FAQ

如何排查用户无法登录IMC服务器管理页面？

查看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。

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>认证设置>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。

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。

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。

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？

设备内将 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。

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。

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。

这个问题并非设备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，设备不可控，故将此问题定位为软件限制，在发布说明书中体现。

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，另一项是设备的 Portal Server 页面配置的超时时间，当 IMC 服务器和设备同时配置超时时间，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，仅在设备的 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。

跨三层环境IMC做第三方Portal认证，用户自动下线，日志显示被管理员踢下线？

跨三层环境下设备上记录的用户 MAC 都是下联三层设备的接口 MAC，而不是用户的真实 MAC，不同 IP 每次上线使用的是同一 mac 地址，IMC 会误认为是同一用户重复上线，导致把用户的超时时间置为 0，设备收到超时时间为 0 的报文后会将用户直接踢下线，在跨三层环境中的 Portal 认证需要开启 SNMP 同步（跨三层 MAC 地址学习）来解决。

31 第三方用户存储认证

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。

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。

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 策略是否错误；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。

32 断点续传 FAQ

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）。

33 特征库升级 FAQ

特征库升级结果中出现“特征库加载失败”？

特征库升级结果中出现“特征库加载失败”，此时是由于内存碎片太多或者剩余可用的内存太少导致，目前已经做了优化，建议在特征库升级时配置自动升级，升级时间配置为流量较小的时间点，例如凌晨零点到两点之间。

34 抓包工具 FAQ

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。

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。

物理接口加入聚合组后，在物理接口抓不到包？

是的，抓包功能是基于软件层面的，接口加入到聚合口后，在软件逻辑上来说不在是独立运行的接口了，因此在抓包时需要选择聚合口来抓取相关的报文。

35 服务质量管理 FAQ

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；

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。

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。

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

在设备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，若是设备通过三层交换机与内网 PC 相连，目前设备没有跨三层 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，任然需要通过认证才能上网。

37 链路负载均衡 FAQ

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。

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。

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。

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，转由其它链路进行负载。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。

优先级定义

基于优先级的是 谁的优先级高先走谁 接口达到阀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。

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。

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。

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。

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。

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 tack 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 新版本链路负载均衡 FAQ

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。

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。

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。

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。

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。

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。

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。

过载保护使用说明？

新版本暂时不支持过载保护功能。

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。

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。

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。

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。

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。

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）。

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**

负载均衡分配不均，未完全按照配置的权重大小比例进行分担？

基于权重负载的负载均衡策略是按照源 IP 地址进行 hash 运算的，当源 IP 数量较少时由于 hash 算法原因查看匹配计数未完全按照配置的权重大小的比例进行负载分担，只有当源 IP 数量较多时才能够与配置的权重大小比例一致。

39 服务器负载均衡 FAQ

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。

权重大小的说明

范围为 1-100。

权值越小，优先级越高。

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。

服务器负载权重匹配说明

负载算法是先根据源地址计算出一个随机数，用随机数对权重和求余数。比如权重配置是是 1:1，加起来就是 2，匹配概率 0 或者 1，当源地址比较少的时候很大概率只能匹配到其中一个服务器。此时需要修改权重值为一个比较大的范围比如是 10:10，匹配概率会变成 1-19，此时负载基本能按照权重匹配（但是匹配数也不太可能完全 1：1，如果源地址范围越大，权重总和越大，就越接近 1:1）。

40 三权分立 FAQ

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。

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。

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不可以修改、但密码可以修改。

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。

三权模式下CLI有配置权限吗？

切换到三权模式后，CLI 的控制权限就被回收了，只有如下命令的权限是放开的"exit","end","en","enable","ping","configure terminal","interface","no shutdown","ip address","save","display running-config","display version","display running-config","allow access" "no admin-switch three-power-mode""debug","log"。

41 广告推送 FAQ

广告对象规格

广告对象配置支持 16 条。

广告策略规格

广告策略配置支持 16 条。

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。

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。

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。

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。

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。

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。

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。

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。

广告策略跨网段使用限制

广告推送如果跨网段推送广告。需要在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）。

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。

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。

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。

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。

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）。

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。

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*3+1 一共 13 秒。

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）。

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。

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。

广告对象图片上传大小

每张图片上传大小最大是 2M。

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。

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。

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。

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。

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。

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。

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。

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。

当新创建的广告对象与之前的广告对象重名时，新创建的广告对象中已经上传的图片被删除？

软件限制，策略重名时图片无法恢复，文字可以保留。

广告策略推送间隔内怎么推送了两次广告？

广告推送配置推送间隔非 0 时，会推送两次，目的是防止非浏览器的 get 报文导致广告推送不出去，虽然目前已有 UA 过滤，尽量避免非浏览器的推送，但做不到完全过滤掉非浏览器的报文。

42 防共享 FAQ

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。

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。

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。

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。

防共享检测方式是否可以不选择？

不可以，至少需要选择一种共享检测方式。

手动惩罚的共享检测用户不会产生共享接入日志？

共享接入日志只有自动阻断或限速的才会产生日志，手动在共享接入监控页面操作栏上手动冻结或限速配置的惩罚用户不会产生日志。

防共享检测方式配置为阻断或者限速，共享检测终端数量达到阈值，是否继续检测？

防共享接入检测如果检测到终端数量已经达到阈值，且惩罚方式配置了阻断或限速，直至超时之前都将不再检测，只有超时之后才会检测；如果惩罚方式配置的是无或者配置了白名单，则达到阈值之后会继续检测。

防共享检测用户达到阈值之后阻断用户，阻断提示有时可以弹出，有时弹不出来？

当内网共享用户达到检测阈值之后，只有访问 http 网页才会有阻断提示，访问 https 网页没有阻断提示，网页无法打开。

43 认证策略 FAQ

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、二维码认证。

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、访客二维码认证其中一种或多种认证方式组合。

版本升级出现配置丢失打印unknown信息？

如从 4.2 或老版本升级到 4.5 版本串口可能打印 user-policy any any any any always permit 1，因为认证方式 permit 已经被删除，或者会打印 user-webauth portal-url default-template，因为新版本认证策略机制修改，该命令已被删除，以前配置认证策略后，需要在认证方式中选择模板类型，目前是认证策略选择单一认证方式就自动关联相应认证方式的默认模板，如果是混合认证，就关联混合模板。

认证策略用户录入使用场景？

主要针对第三方用户，目的是将存在于第三方的用户加入设备，便于做策略限制等。此功能不影响本地已有用户，只会新增用户，不会修改已有用户信息。

认证策略用户录入未配置时认证用户的处理？

认证策略用户录入未配置用户组时不会录入用户。

第三方录入用户，如果用户未下线，用户的处理？

第三方录入用户，如果用户未下线，该用户无法编辑，在线用户注销后，用户可以编辑。

认证策略录入用户有效期录入，有效期过期后用户的处理？

认证策略有效期录入用户，当认证策略里用户有效期过期后用户状态变为未启用状态，如果重新启用用户的话需要更换用户有效期为有效时间。

认证策略录入用户有效时间的三种方式？

第三方用户认证录入支持永久录入、有效期录入、临时录入。

(1) 永久录入：指用户认证成功后录入到设备的用户不会自动删除，未删除的情况下长期有效；

(2) 有效期录入：是指用户认证成功后录入到设备的用户到达指定日期后录入用户和该条认证策略都失效，如果启用需要修改时间在有效范围内。

(3) 临时录入：是指用户认证成功后录入用户到设备指定的用户组，当用户注销下线后，录入的临时用户会自动删除。

认证策略临时录入用户命令行clear user-recognition？

临时录入策略命令行 clear user-recognition，录入用户不会删除，需要手动删除用户。

用户认证性能优化支持哪几种认证方式？

本地 web 认证、ldap 认证、radius 认证、微信认证均已支持用户态性能优化，其它认证方式仍然在内核态实现，认证性能没有变化。

配置Portal Server认证方式的用户录入，当imc配置推送用户组时与设备配置用户录入到用户组哪个优先？

为了保证原有功能不受影响，优先录入到 imc 配置推送的用户组中，功能与以前保持一致，当用户进行 Portal Server 认证，认证成功后，用户会被录入到设备配置的 imc 推送的同名用户组中，用户下线后，录入到 imc 推送用户组的用户会被删除。

44 认证模板设置 FAQ

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、二维码认证的弹出 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。

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。

45 短信认证 FAQ

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。

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。

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。

46 免认证 FAQ

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。

47 无感知认证 FAQ

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。

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。

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。

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。

如果本地认证的用户信息在 LDAP 和 Radius 服务器上，LDAP 的用户需要同步到设备本地或认证策略里配置录入用户。由于 Radius 的用户不支持同步，故 Radius 用户认证需要认证策略里配置录入用户。

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。

HA主机上本地无感知上线的用户不会同步到HA备机？

目前无感知上线的用户暂不支持 HA 同步，因此 HA 主设备在线用户显示无感知认证上线的用户名，而 HA 备机上显示的是匿名用户。

48 访客二维码认证 FAQ

二维码认证功能应用场景有哪些？

访客二维码认证主要针对下列两种场景：

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

需要弹出审核页面，直接以审核人身份上网。

审核人配置的是any，为什么我的手机无法进行审核操作？

在二维码访客认证页面中的审核员为在线认证用户，any 代表所有在线的认证用户，匿名用户或非在线认证用户不行。

49 混合认证 FAQ

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，混合认证支持微信认证、短信认证、本地认证、免认证、访客二维码认证其中一种或多种认证方式组合。

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，同时也选择多种的认证方式。

混合认证的模板和其它认证一样吗？

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

50 用户源 MAC 日志显示 FAQ

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。

51 https 弹 portal FAQ

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。

安卓手机https弹porta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。

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，以便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。

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。

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。

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。

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。

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。

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**。

用户https弹portal通过认证后不支持自动跳转？

https 网站是加密的，无法实现自动跳转或跳转到指定的重定向 URL，包括由于访问 https 网站被策略阻断后也无法推送阻断提醒页面。

52 伪 Portal 抑制 FAQ

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。

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。

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。

53 地址本域名 FAQ

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，并支持在其它策略中引用。

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。

54 NAT44 FAQ

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。

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。

NAT44是否支持ALG？

NAT44 暂不支持 ALG，可以用源 NAT 功能配合 ALG 使用。

55 4G 上网卡 FAQ

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。

56 PPPOE 拨号 FAQ

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。

57 用户/用户组 FAQ

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。

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。

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。

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。

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）。

user-group有限制但是依然可以使用受限制的特殊字符。比如：！￥。。。。。？

由于命令行下输入的中文字符类型可能是 UTF-8,可能是 ANSI,也可能是其它的编码格式，而且中文字符是 2 个 char 型，不同类型的编码是不一样的，这个无法进行限制，如果对其中的一种编码的中文字符做了限制，但是在其它的编码中可能并不是异常字符，这样限制就会有问题，因此目前命令行对以上中文非法字符未作处理，目前很多模块由于此种情况均存在未对中文特殊字符进行检查。

用户组最多支持几级？

在用户组织结构下用户组最多可以建 8 级。

用户排除地址提交总是提示不合法？

配置的排除地址必须要在绑定范围内才会生效，否则提示排除地址不合法。

引用用户规格是多少？

其它模块引用用户最多引用 64 个用户对象。

属性组如何导出

在根组导出组织结构，会导出所有用户和用户组，但是不包括属性组，点击属性组后导出的为属性组。

在线用户中哪些认证方式会在认证用户组中创建用户组？

- 本地认证不会新建用户组；
- 静态绑定 ip 和静态绑定 mac 不会新建用户组；
- portal 认证会新建用户组：portal-server 用户；
- 短信认证会新建用户组：短信用户；
- 免认证会新建用户组：免认证用户；
- 微信认证会新建用户组：微信用户；
- 混合认证会根据用户选择的哪种认证方式认证后进行创建不同的组，认证方式为选择的认证类型方式；
- 二维码认证会新建用户组：二维码用户；
- 单点登录会新建用户组：单点登录用户；
- IMC 推送 UDP9999 会新建用户组：IMC 用户，所属组 IMC 用户，认证方式为 imc；
- 第三方 radius 用户认证会新建用户组：Radius 用户组，认证方式为第三方 Radius 认证；
- 第三方 ldap 用户认证会新建用户组：Ldap 用户组，认证方式为第三方 Ldap 认证。

用户组下最多允许多少个对象？

根据不同硬件类型，每个组下最多允许对象也不一样，但是在默认组下允许对象数没有限制，但也不会超过最大规格。

用户导入时导入用户不全

如果在导入时有用户被引用，会出现导入不全的情况，因为导入的时候是先删除用户再导入用户，而被引用的用户，是无法被删除的，此时出错，那么退出，故导致导入不全。存在此情况时建议使用“跳过，不导入该用户”的方式

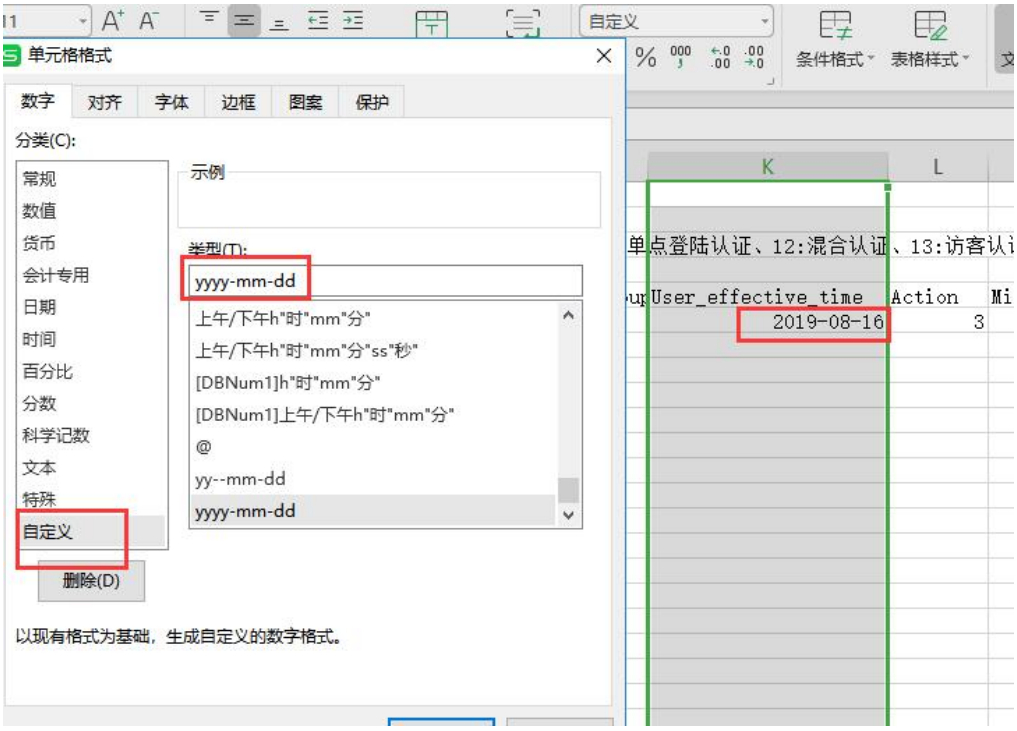
认证策略中，导入认证策略与创建的策略的用户有效时间格式不一致？

目前我们设备使用的 yyyy-mm-dd 的风格进行显示。

csv 的源文件使用 Notepad++打开显示的也是 yyyy-mm-dd 风格。

```
"### (2) Action:认证方式（2:微信认证、3:Web认证、4:Portal认证、8:短信认证、9:免认证、10和11:单点登陆认证、1
"### (3) Mix_auth_flags:混合认证方式（上述几种认证方式随机组合）",
"ID","Status","Name","Desc","Ifz_in","Ifz_out","Src","Dst","Sche","Usergroup","User_effective_time","Action
"1","enable","1","","any","any","any","any","always","","2019-08-16","3","0",
```

csv 默认使用 Excel 打开时间显示类型为 yyyy/mm/dd，可以修改时间的显示格式，修改为 yyyy-mm-dd，如下图所示：



58 用户同步 FAQ

用户同步规格

LDAP 同步条目 128，SNMP 同步规格 64，ARP 扫描条目 64 个。

LDAP用户录入

LDAP 同步录入用户不支持指定用户组，录入按照 AD 域上 OU 和安全组进行录入。

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。

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）。

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。

LDAP同步绑定方式？

LDAP 仅支持简单模式的联动认证，不支持匿名和通用模式的联动认证。

LDAP同步支持的服务器？

E6442 及以上的版本，支持与 Openldap、Windows AD 域服务器的认证对接。

LDAP同步用户的限制?

AD 服务器上用户名超长(大于 63 字符)，含有异常字符（汉字数字字母以及@._-()[]|以外的特殊字符）可以同步，不能录入到本地用户结构，同步过程中会依次在本地用户结构添加用户、用户组，本地满规格时无法录入，同步规格和本地用户规格相同。

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。

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。

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。

IPSec和SSLVPN使用LDAP认证？

IPSes 和 SSLVPN 条件下使用 LDAP 认证时，IPSes 和 SSLVPN 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。

LDAP同步周期？

LDAP 同步周期起始时间（0-23），间隔时间（1-24），例如起始时间 8，间隔 2，代表该同步条目每天 8 点开始同步，每隔 2 小时同步一次，晚上 12 点结束当天的同步任务。

多个用户同步任务并存时处理？

多个用户认证并行时，用户同步任务单线程处理，上一个同步任务完成后，才开始下一个同步任务。

使用AD域用户认证，修改Ad域上密码后，认证使用旧密码还可以认证？

AD 域用户更新密码后，使用同步的 ldap 认证时，新旧密码都可以认证。在 server 2008 级别的 AD 下，旧密码生存期为 5 分钟，在 server 2003 级别的 AD 下，旧密码生存期为 60 分钟。

这个 5 分钟就是为了防止 AD 同步延时问题，防止 DC 数量比较多时，用户登录所在的站点内还没有成功的更新到密码的修改的情况。这样，即使新密码没有生效，旧密码依然可用。

测试 2003 的服务器，旧密码有效期为 60 分钟，自测 60 分钟后密码失效，此为 AD 域服务器的保护机制，不修改。

LDAP同步用户处理？

手动创建用户组、用户创建为本地用户，和 ldap 服务器上组、用户名称一样，点 ldap 同步，这个用户没法用 ldap 认证，ldap 同步当存在重名用户时，只移动用户，不覆盖。

LDAP组认证处理？

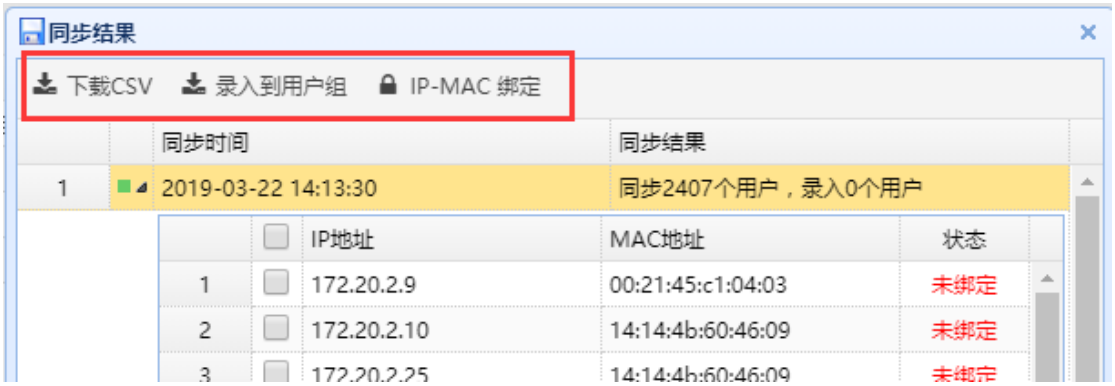
ldap 组里第一个 ldap 服务器密码不对，用户在第二个服务器，此时用户认证浏览器无响应，目前处理不了跨域的 ldap 组认证，需要保障 ldap 组下地址可达，服务器密码正确。

ARP扫描网段限制？

arp 扫描只支持扫描设备同网段用户。

ARP扫描和SNMP用户录入？

arp 扫描和 SNMP 录入支持指定用户组录入和不录入，如果配置的 ARP 扫描和 SNMP 同步未指定录入组，只扫描同步，录入用户。可以在同步结果页面，直接下载 CSV 文件、录入到指定用户组、支持 IP-MAC 绑定。



SNMP同步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。

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 SNMP 同步后，交换机下的新用户 IPMAC 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。

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。

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。

每次SNMP同步结果如何处理?

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。

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。

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。

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。

在认证页面用户主动注销之后，在原来认证界面重新使用别的用户认证登录出现不录入？

因为录入前没有流量做策略匹配导致获取不到录入的组，因此无法录入，这种情况需要用户重新弹认证页面上线才能够正常录入。

radius和ldap认证服务器，点击测试有效性是如何进行测试的？

radius 服务器是使用 icmp 检查，如果有回复则认为成功，ldap 服务器是使用协议默认的 tcp 389 端口进行测试，并且会使用配置的管理员及密码进行验证，验证通过后才认为成功。

59 端口镜像 FAQ

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）。

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。

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。

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。

是否支持远端镜像功能

不支持，由于设备仅仅支持单台模式，因此仅仅支持本地镜像，而不支持远端镜像。

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。

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。

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。

60 解密策略 FAQ

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。

电脑端证书如何导入？

电脑端需要安正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】。

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。

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。

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。

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-设备 1-设备 2），设备 1 证书为 mm.cer，设备 2 证书为 https.cer，用户电脑应该导入设备 1 的证书 mm.cer。

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。

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。

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。

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。

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。

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。

开启解密策略，手机安装证书后仍然一直提示不安全，点击继续后仍然会一直弹安全告警？

需要在命令行配置 sslproxy serial-random disable，由于 ssl 客户端生成的证书的序列号为服务端证书+随机数计算而成，每次序列号是变化的，对于某些手机端的浏览器安装了证书还是会存在合

法性校验验证不过，会被浏览器拦截，这个时候如果弹出了继续浏览按钮，点击继续浏览，下一次 ssl 握手推送的证书和上一次证书的序列号不一致，还会被浏览器继续拦截，因此会一直弹告警，但是在配置了 sslproxy serial-random disable 后，会每 10 分钟变化一次随机数，这样点击继续浏览后两次的证书序列号是一致的，就不会存在一直弹安全告警了。

同一目的IP的不同域名的HTTPS流量，只要有一个域名在HTTPS对象中且解析了域名IP，另一个域名的HTTPS流量在没有建立HTTPS对象的情况下仍然可以进入解密流程。

是的，目前解密中的域名地址的匹配是通过监听 DNS 报文解析出 IP 地址，然后以此地址和目的地址进行匹配的，因此如果两个不同的域名绑定了相同的 IP 地址，只在 HTTPS 对象中配置了其中一个域名，另一个域名也是会进入解密流程的。

61 限额策略 FAQ

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。

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。

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。

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。

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。

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。

用户被阻断后限额的流量统计仍然会增长？

流量阻断后，用户产生的流量过设备仍然会进行统计，从另一方面可以帮助管理员判断是否有攻击或用户电脑是否中断一直产生异常流量。

限额策略配置修改后，统计数据不会清零？

限额策略配置修改后统计数据不清零，会在之前的基础上继续累加，如果希望将某个用户的统计数据清零可以在限额用户统计页面删除指定用户。

月限额统计日期实现机制？

起始日期配置后，月限额定时器会启动，然后定时判断当前时间是否超过配置的时间，如果没有超过，限额会一直统计累加，如果超过当前配置的起始日期，就会把上个周期的统计清零，修改起始日期不会把之前的统计清零，会继续在之前的基础上累加的。

限额统计支持配置恢复？

限额统计支持设备重启后恢复的机制，限额用户的统计数据会定期（1 个小时）写到文件中，下次设备重启后，会从文件中读取之前的记录，避免设备重启后，限额统计被清零的情况。

限额用户统计在线时长与认证用户实际在线时长不一致？

限额统计是基于用户流量触发来统计在线时长，无流量不统计，与认证用户实际在线时长没有关系，是两个维度，避免认证用户在没有使用网络的时候也会被统计在线时长，出现严重统计误差（如永不超时）

不在限额策略源IP范围内的用户也会匹配上策略？

是的，针对 UDP 流量不在源 IP 指定范围内时也能匹配上限额策略，因为 UDP 流量无法区分正反向，所以在匹配时会将流上的源目 IP 调换一下跟匹配条件对比一次，即做了双向匹配，避免下行流量先过设备时永远无法匹配上策略。

62 DDNS 功能 FAQ

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。

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。

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。

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。

63 DNS-DNAT 功能 FAQ

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。

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。

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。

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

64 多配置管理功能 FAQ

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。

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。

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。

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。

导入配置文件进行配置恢复，设备重启过程中不能选择配置保存？

导入配置文件进行配置恢复时，设备重启过程中配置保存选项要 N，不能输入 Y，否则设备的运行配置会覆盖导入的配置文件，导致配置恢复失败。

65 Portal 逃生 FAQ

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。

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。

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。

portal逃生存储用户数达到规格时设备如何更新？

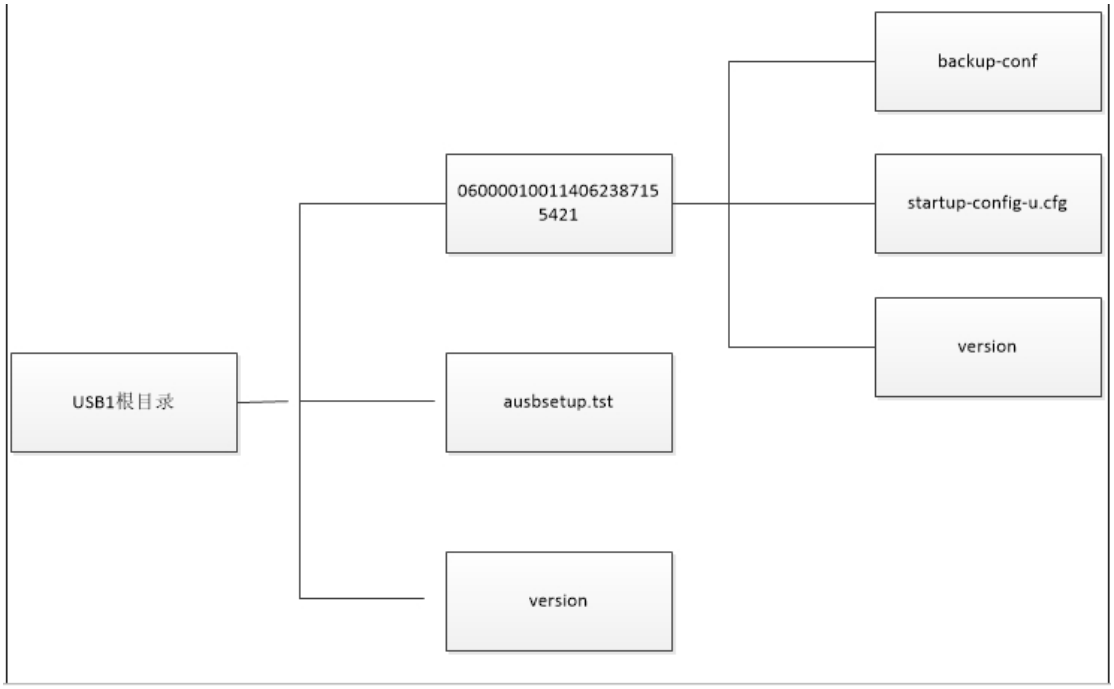
认证用户有保存用户数的规格限制，当存储用户数达到规格时，优先删除最久没有流量的用户。

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 trach 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）。

66 零配置上线 FAQ

零配置启动盘格式？



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。

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。

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。

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。

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，**display log debug** 即可看见日志。

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。

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。

67 审计日志导出 FAQ

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。

审计日志包括哪些类型？

包括访问网站日志、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、其它应用日志。

审计日志导出支持附件内容导出吗？

不支持，比如邮件日志里的内容和附件就不支持导出。

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。

审计日志有规格限制吗？

有，户导出的最大日志大小为 25 万条左右（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。

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。

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来的是其它日期的日志？

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。

日志导出不支持基于查询条件导出？

不支持按查询条件导出，审计日志、系统日志、操作日志、网络层安全日志等均不支持基于查询条件导出。

68 业务告警 FAQ

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。

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。

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。

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。

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。

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。

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。

69 应用自定义 FAQ

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。

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。

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。

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。

自定义应用没有审计日志只有阻断日志？

自定义应用不支持审计，因为每一种应用的审计日志都是需要通过事先分析应用中的特征来提取出对应的审计规则才能正常产生审计日志，对于自定义应用由于只是根据 IP、端口、URL 等规则做简单的流量识别，所以无对应的审计规则，无法产生审计日志，自定义应用阻断日志同其它所有预定义应用的阻断日志一样发送到应用控制日志中。

70 中英文切换 FAQ

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。

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。

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。

71 用户标签 FAQ

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。

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。

标签规格

预定义只有 56 个，不支持手动创建自定义 url 分类，其它的 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。

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。

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））。

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。

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。

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。

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。

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。

用户标签启用禁用

User-lable enable

User-lable disable

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
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

分类 ID	中文名称	英文名称
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
50	外汇	exchange
51	旅游	travel
52	暴力	violence
53	病毒	virus
54	WEB通信	web-im

分类 ID	中文名称	英文名称
55	交通住宿预定	hotal
56	白名单	whitelist

72 AD 域单点登录 FAQ

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。

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。

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。

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。

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。

73 无线非经 FAQ

升级最新非经版本之后，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。

开启无线非经功能之后，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：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。

无线非经普通内容日志显示包含格式类字符？

目前特征提取是从格式开始的地方开始提取的，一直到结束为止，目前包含内容的日志都是这种方式处理的，修改涉及范围较大，后续版本统一优化处理。

英文管理页面下不显示无线非经配置？

是的，目前无线非经的功能只是在国内存在，因此在英文管理页面下是不支持也不展示无线非经的相关匹配的。

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。

开启无线非经功能之后，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）。

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。

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 字段与设备上的未匹配上，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。

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。

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。

sftp上报配置一台未开启SFTP服务的IP地址上进行数据上报，命令行使用display wireless-count查看上报计数有统计

由于获取不到 sftp 上传失败的信息，因此目前在上传失败后相应的命令查看信息仍能看到相关的统计。

非经配置导出修改后再导入提示信息中的信息显示不准确？

由于非经字段非常多，检查很复杂，有些特殊字段是动态生成或拼接而成，无法实现精确检查，所以不能保证提示信息 100%准确，比如当配置导入时检查完所有的行和列确认类型配置没有问题后会记录最后一次检查的行列值作为提示返回，但由于修改的字段，长度拼接后出现超过范围的情况，此时的提示信息会用之前的行列值加上字段错误的信息返回，这样就造成了提示信息中的行列值并不是真正有问题的字段，出现不准确的情况。

74 WEB 页面提示格式化硬盘

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八本，打开 WEB 会提示格式化。

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。

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。

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。

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。

75 全局配置 FAQ

两种识别模式的区别是什么？

识别模式分为“启发模式”和“强制模式”两种，默认配置为强制模式，识别范围默认配置均为 private 私网地址段。

“启发模式”指的是，优先将属于识别范围的 IP 地址识别为在线用户，并且根据流量发起方先识别源 IP，再识别目的 IP，如果源 IP 和目的 IP 都不在识别范围中时则将源 IP 识别为在线用户。

“启发模式”使用场景：对用户识别要求不严格的情况下使用启发模式，在线用户中会出现非识别范围内的用户（如：同时出现私网 IP 和公网 IP 的用户），所以统计到的在线用户数量会比较多，在此模式下需要将识别范围修改成内网实际使用的地址网段，否则会导致用户识别不精确。

“强制模式”指的是，只将属于识别范围的 IP 地址识别为在线用户，并且根据流量发起方先识别源 IP，再识别目的 IP，只有源 IP 或目的 IP 地址中的一个属于识别范围时，才会被识别为在线用户；否则此 IP 地址流量不受系统转发流程中用户识别后的所有功能模块限制，如：用户策略、安全策略、应用识别和审计、入侵检测、病毒防护、QOS。

“强制模式”使用场景：对用户识别要求严格的情况下使用强制模式，在线用户中只会存在识别范围内的用户，过滤掉了不属于内网地址段的用户，精简了在线用户列表，只显示用户真正关心的数据，同时提升了设备性能，不在识别范围内的 IP 流量不走用户认证流程，避免了对用户不关心数据的处理，在此模式下务必将识别范围修改成内网实际使用的地址网段，避免因识别范围配置错误导致的用户关心的 IP 地址流量不受用户策略控制的情况出现。

76 第三方用户同步

pppoe未开启更新网关更新dns，第三方pppoe监听用户不上线？

由于在开启更新网关后，会在设备中增加一条默认路由出接口是 ppp 口，这样很容易就会有 ip 流量通过 ppp 接口发送出去，第三方 pppoe 监听用户上线需要收到协议 0x8864（pppoe 协议）并且是 0x0021（ipv4 协议）的报文，获取到 ip 地址，然后根据 session id 和源 mac 进行查找其关联的用户名进行上线，如果在不配置更新网关的情况下，可通过 ping 对端 ppp 接口地址手动触发（可通过 display ip route 查看到 ppp 接口对端 ip 地址），此时报文走 ppp 接口发包，也会触发 pppoe 第三方用户上线。因此该现象与配置更新网关和更新 dns 并无直接关联，只要 ipv4 流量走 ppp 接口发包，pppoe 第三方用户就能获取到 ip 信息上线。

本地用户与第三方录入用户同名时，第三方同名用户上线后，本地用户无法编辑、删除？

WEB 用户同步录入用户与本地用户同名时，第三方用户同步的 WEB 用户同步上线后，由于户管理模块未区分是录入的用户还是本地创建的用户，该同名用户就会变成已经被引用的用户，此时本地用户中的该同名用户不可编辑和删除；只有把第三方 WEB 同步用户注销后，本地用户中的同名用户才能进行编辑和删除。

77 在线用户 FAQ

在线用户冻结是否支持IP维度？

在线用户冻结是基于用户维度的，不支持 IP 维度。

在线用户踢除是否支持IP维度？

在线用户踢除支持基于 IP 维度。

78 SSL VPN FAQ

为什么通过SSL VPN拨入后，无法访问该设备的WEB页面？

默认不允许通过 ssl vpn 隧道管理本机，可通过配置视图下敲 **ssl vpn allow access { all | center-monitor |http | https |ping | ssh | telnet }**命令来允许 sslvpn 隧道管理本机。

VPN客户端都支持哪些操作系统？

客户端支持所有的 win7 和 win10，Android6.0 以上手机。

为什么客户端主动下线后，此时查看设备端，发现此用户还在线？

客户端自己断开或者在设备上注销，都不会发送下线消息给对方，VPN 断开连接是自己的探测机制，每 10S 发送一次加密报文，客户端 120s 内没收到服务器的探测信息，自己下线。设备端 150s 内没有收到客户端的探测信息，注销在线用户。

为什么资源里放通FTP服务后，客户端还是无法下载FTP资源？

资源如果选择 FTP 协议，不支持被动模式。如果支持，再设置自定义 tcp 端口 1024-65535。

SSL VPN客户端因为未分配到IP地址拨号失败，但设备上会显示此在线用户？

是的，SSL VPN 客户端先执行的登录认证，之后再给客户端分配 IP 地址，在客户端认证成功后会记录设备在线用户，但是客户端因为未分配到 IP 地址所以拨号失败，由于无法成功拨号，也就无法正常发送心跳报文，因此在 2 分钟后，SSLVPN 在线用户会自动老化消失。

用户配置了初次认证修改密码，SSL VPN使用此用户上线后不需修改密码？

是的，由于初次认证修改密码是需要设备主动进行页面访问来推送弹窗，但 SSL VPN 客户端的认证流程无法进行弹窗，因此 SSL VPN 使用此用户上线后是不会强制修改密码的。

SSL VPN资源如果被策略引用，在进行导入的时候不会进行覆盖修改？

是的，目的是为了防止误导入影响正常 SSL VPN 的使用，因此被策略引用的资源是不进行覆盖修改的。

配置证书登录时，客户端无法通过证书校验

(1) 本地证书和对端证书必须是 CA 证书签发，客户端否则无法通过证书校验。

(2) 本地证书或对端证书失效后，客户端无法通过证书校验。

本地证书和对端证书导入了已注销的证书，为什么客户端可以通过证书校验？

本地证书和对端证书如果导入已注销的证书，若 CA 证书正确的情况，客户端依然可以通过证书校验，设备无法针对证书是否注销进行判断。

SSL VPN资源的导入导出文件中Type的值表示的含义

Type 的值表示 SSL VPN 预定义的资源类型，显示为十进制的值，是由二进制转换过来的。资源类型的二进制值是按照资源类型对应的二进制位置进行置位标记的，第一位是 HTTP，第二位是 HTTPS，第三位是 FTP，第四位是 ICMP，第五位是 SSH，第六位是 TELNET，第七位是邮件（SMTP，IMAP，POP3）；置 1 表示允许，置 0 表示不允许。比如资源类型配置为 HTTP 和 SSH，即为 0010001，转换为十进制数即为 17；如果资源类型为 any 或者自定义的，Type 的值为 0。

79 虚拟网线 FAQ

虚拟网线不能配置IP，如何通过页面管理设备？

需要在其它未使用的接口配置 IP 地址用来管理设备。

配置虚拟网线后，用户认证、防共享功能还能使用吗？

可以正常使用，认证用户和设备管理口要路由可达，不然会出现认证页面无法打开的情况。

80 旁路认证 FAQ

旁路认证默认状态是什么样？在哪里开启？

旁路认证默认状态为关闭状态，需要在部署方式高级配置开启此功能。

旁路认证的用户认证策略如何配置？

在用户认证策略中配置的源接口以及目的接口必须配置接收镜像流量的旁路部署接口或者是 any。

旁路认证时，没有匹配到源地址也会弹认证页面？

旁路认证为双向认证，源地址配置是 PC 访问的目的 IP 地址也会弹出认证页面。

旁路认证时，用户302重定向页面无法打开

当配置好旁路认证后，用户访问 http 网页，向重定向页面跳转时，能跳转 URL 但是页面无法访问，要确保旁路设备到上网 PC 要可达，故旁路认证务必保证旁路设备到上网 PC 可达，否则功能无法使用。

旁路认证不支持哪些认证方式？

旁路认证对 http 报文返回 http 302 重定向报文，让用户访问认证服务器，认证服务器弹认证页面给客户端。

旁路认证对 https 报文直接发送 tcp reset 报文进行阻断。

81 旁路阻断 FAQ

旁路阻断默认状态是什么样？在哪里开启？

旁路阻断默认状态为关闭状态，需要在部署方式高级配置开启此功能。

旁路阻断控制策略应该如何配置？

在 ipv4 控制策略中配置控制策略为拒绝，并且配置源接口以及目的接口必须配置接收镜像流量的旁路接口或者是 any。

配置好旁路阻断后访问外网页面无提示。

控制策略中配置行为为拒绝时，PC 无法正常打开外网页面，无提示；如果是 url 控制或应用控制中配置拒绝会弹出提醒页面。

配置好旁路阻断后还是可以ping通外部地址

旁路阻断只针对于 TCP 报文生效，对于 UDP，ICMP 等报文无法进行阻断。

配置好旁路阻断后能正常访问外网

对 TCP 报文的阻断由于是发送 reset 进行阻断，如果存在外网流量回复速度快于旁路设备发送的 reset 报文速度，那 pc 将能够正常打开外网正常上网。

测试PC到旁路阻断设备不可达，功能生效吗？

旁路阻断务必保证旁路设备到上网 PC 可达，否则功能无法使用。

82 管理员外部认证 FAQ

管理员外部认证对哪种模式生效？

管理员外部认证功能只针对管理员模式生效，三权模式不支持。

管理员外部认证能选择几个服务器对象？

外部认证时，只支持选择服务器对象且只能选择一个，不支持同时选择多个，不支持服务器对象组，与系统创建的管理员保持一致。

配置管理员外部认证关闭服务器异常开启本地认证会有什么后果

如果关闭服务器异常开启本地认证后，当设备与外部服务器无法通讯时，管理员将无法登录设备，所以请慎重选择是否需要关闭服务器异常开启本地认证。

如果开启服务器异常开本地认证，当设备与外部服务器无法通讯时，使用设备本地管理员可以登录管理设备。

使用管理员外部认证，使用服务器账号无法登录设备

服务器管理员账号可能没有限制，允许所有的特殊字符，并且账号长度没有显示，因此在登录设备时设备对外部服务器登录账号格式也有校验，故此在外部服务器创建登录账号时要符合设备管理员账号要求。

83 热补丁 FAQ

允许最多上传几个热补丁？

上传热补丁数量限制为 5 个，上传第 6 个的时候会给出相应报错提示。

允许连续对热补丁进行操作吗？

为了保证补丁操作进程堆栈安全，补丁的操作时间间隔为 30S。

对已经加载热补丁进行升级版本操作，热补丁内容如何处理？

热补丁升级版本，会将当前版本上所有的补丁文件删除，当前补丁不卸载，当设备重启后，加载新升级的版本。

主备模式下热补丁如何给备机加载热补丁？

在主机上操作热补丁会同步到备机上，例如：在主机上传、加载、卸载和删除热补丁操作均会同步到备机上。

84 统计报表 FAQ

新建报表任务时报表格式有些设备只显示html格式，有些显示pdf和html两种格式？

1G 内存设备报表格式只支持 html 格式，2G 及 2G 内存以上设备报表格式支持 pdf 和 html 两种格式。

统计报表模块有些设备能显示，有些设备不显示？

统计报表模块依赖于设备硬盘，只有在有硬盘的设备上才会显示，没有硬盘的设备上将不会显示统计报表模块功能。

统计报表中的数据不准确存在异常不符的情况？

目前的报表统计流程是：

(1) 制作报表

(2) 更新记录（报表占用空间使用率数据更新）

(3) 数据汇聚（从内存中获取会话数、CPU、内存使用率状态信息存入数据库中）

(4) 休眠 5 分钟

以上 4 个步骤循环。

有两种情况会影响报表统计的数据不准确：

(1) 设备运行异常、当 CPU 和内存使用率很高时，可能会导致读取会话数、CPU 和内存使用率的数据失败或入库失败导致数据缺失或入库数据不准确。

(2) 当系统繁忙，数据汇聚时间过长时（比如 2 个小时），会导致这段时间的会话数、CPU 和内存使用率数据获取不到（数据汇聚时不会从内存获取会话数、CPU 和内存使用率的数据），这样就会导致后续数据汇聚时存在数据缺失。

报表中的CPU利用率统计和UI上的统计不符？

主要是由于采样以及数据分区划分的原因：

(1) 采样原因：UI 上的统计采样是分布均匀的；报表中的采样分布不均匀，报表数据采样时由于需要处理很多数据的汇聚，所以每次采样的间隔时间都不同；

(2) 数据分区：UI 上的统计是按照时间进行数据分区，然后每个分区取均值；统计报表数据是根据采样数据的记录条数来分区的，每个分区数据量=采样数据总数/分区数，这样计算出来的分区数据无法跟显示时间对应，所有造成 UI 统计显示与报表统计显示不一致。

HA主备环境下使用手工同步，不同步历史报表？

是的，点击手工同步会同步报表管理中的配置，不会同步历史报表中的文件，同时 HA 监控中的系统配置会显示两端配置一样，不会对比历史报表是否一致。

统计报表中CPU利用率统计的信息与实际情况不符？

报表中的 CPU 利用率统计和 UI 上的统计不符主要是由于采样以及数据分区划分的不一样。

- 采样原因：UI 上的统计采样是分布均匀的；报表中的采样分布不均匀，报表数据采样时由于需要处理很多数据的汇聚，所以每次采样的间隔时间都不同；
- 数据分区：UI 上的统计是按照时间进行数据分区，然后每个分区取均值；统计报表数据是根据采样数据的记录条数来分区的，每个分区数据量=采样数据总数/分区数，这样计算出来的分区数据无法跟显示时间对应，所以造成 UI 统计显示与报表统计显示不一致。

85 全局白名单

如果源地址既是白名单又是黑名单如何处理？

白名单优先级高于黑名单，按照全局白名单走，不去匹配黑名单。

设备上配置了全局白名单，但该用户仍会匹配上网行为相关策略？

只有会话中源地址配置了白名单，才会走白名单流程，不匹配上网行为相关策略。

在全局白名单中使用ip地址进行搜索时为什么没在配置ip地址范围内的ip也会搜索出来？

白名单查询支持模糊匹配，没有进行名称、地址、描述的区分。

在全局白名单中配置地址为mac地址时，ipv6控制策略中配置为拒绝时仍然会被阻断？

是的，目前全局白名单不支持 IPv6 相关策略，且全局白名单中也不支持配置 ipv6 地址。

86 公告页面 FAQ

是否支持上传公告页面？

支持上传公告页面功能，但上传页面文件不能超过 2M，文件格式见默认模板。

编辑公告页面时，是否可以支持插入图片、文件及链接？

编辑公告页面时，可支持插入图片、文件及链接，但是所有资源不能超过 2M。

编辑公告页面时，无法提交成功，提示页面超过2M，如何删除导入的图片、文件？

页面超过 2M 后，需要到文件（图片）服务器里删除，然后再提交。

87 移动终端管理 FAQ

为什么配置移动终端管理冻结策略，内网PC并未被冻结？

移动终端管理策略只控制移动终端和多终端用户，不控制 PC 端用户。

移动终端识别的方式有哪些？

移动用户识别，通过 UA（移动终端访问网站是带的字段）和应用特征来识别移动终端用户。

88 应用智能识别 FAQ

迅雷智能识别两种级别宽松度有什么区别？

“严格”是特征+多线程识别方式，“宽松”是使用多线程识别方式，有误报的可能。

P2P智能识别三种级别宽松度有什么区别？

P2P 智能识别，是针对 UDP 流量进行固定特征+并发连接识别方式，“严格”和“适中”都是先进行并发连接识别，再进行固定特征识别，“严格”要求并发连接阈值高。“宽松”是固定特征识别方式，有误报的可能。

应用智能识别是什么功能，是否能保证迅雷应用和P2P应用的100%识别？

此功能是对迅雷及 P2P 行为识别的加强，优先特征识别，在特征未识别出来的时候才会走到此智能识别，由于迅雷及 P2P 应用的复杂及特征多变性，不可能做到 100%准确识别，只能通过此功能来提高识别率，p2p 行为的智能识别，是针对于 udp 流量，当一条流前 20 个包未识别出具体应用时，做 p2p 智能识别，设备中有一个端口配置文件，记录一些常见 P2P 应用的端口，此文件是随特征库一起升级更新的，主要支持以下常见的 P2P 应用（这些不能保证 100%准确，随着其版本的更新可能会有变化，如果发生变化，我们更新相关配置文件即可，版本不需修改）

(1) P2P 软件支持：脱兔、快车、utorrent、比特精灵、比特彗星。

(2) P2P 流媒体（客户端）支持：优酷、芒果 TV、芒果 TV、YY 直播、腾讯视频、爱奇艺、PPTV、搜狐视频。

迅雷的应用很复杂而且有些还是加密传输的，可能会出现识别流量不全或未识别的情况，比如某些特征改变或者其报文加密算法变更，将无法识别出来，这些并不是版本功能问题，可通过更新版本特征库解决。

89 告警功能 FAQ

告警功能里的邮件配置第一个配置QQ邮箱时，会出现收不到告警邮件？

这个是由于发送到 qq 邮箱的邮件较多时，QQ 邮箱服务器会认为是垃圾邮件不接收给打回，导致邮箱收不到告警邮件，出现此问题时可通过开启 debug smtp-client 查看到如下 debug 信息进行确认：554 DT:SPM 163 smtp5,D9GowABXb3Mszp1cV60HAA--.10S2 1553845804,please see http://mail.163.com/help/help_spam_16.htm?ip=220.249.52.178&hostid=smtp5&time=1553845804。

90 资产管理 FAQ

资产管理功能使用场景？

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

资产支持几种识别方式？

通过流量发现、端口扫描、手动添加方式添加资产，其中流量发现、端口扫描加入的资产需要配置资产识别设定范围。

为什么资产管理已经有资产信息，但是在资产安全分析未展示数据？

资产管理中资产信息是实时数据，而资产安全分析中是汇总数据，15 分钟汇聚一次，因此存在时间差。

HA环境下，为什么部分资产未同步到备机？

资产管理只会同步手动添加的，自动发现的不支持同步，导入的所有资产可支持同步至备机。

资产管理中，为什么有资产是活跃状态，有资产是空闲状态？

活跃状态代表资产在线，若一个小时内资产没有更新，则认为是离线设备，页面展示为空闲状态。

资产管理满规格后，如何处理？

资产管理，无硬盘设备，支持 5000 规格，有硬盘设备，支持 5W 规格，达到规格后，只支持更新不支持新增。

资产管理的导入导出文件中属性状态这一列的数字表示的含义

属性状态列的数字用来标识操作系统、部门、用户名是否为用户自定义，第一位为操作系统是否自定义标记，第二位为部门是否自定义标记，第三位为用户名是否自定义标记，如果是自定义的就为 1，不是自定义的就为 0，然后转换为十进制数进行显示，比如用户名和部门是自定义的，操作系统不是自定义的，那就是二进制的 110，转换为十进制数即为 6。

91 接口及其它 FAQ

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。

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。

物理口加到安全域后无法加入到聚合口？

是的，加入到域的物理口是无法加入到聚合口的，同样如果物理口加入到聚合口后也就无法再将此物理接口加到安全域了。