AG-6000 融合应用网关

技术白皮书

版权声明

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京安博通科技有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京安博通科技有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

目录

1 概述

信息和网络技术的发展，让互联网已经渗透到了社会生活每一个角落；不仅成为人们学习、生活的重要工具，也成为了企业高效运营、开放的基础平台。伴随着 Web 2.0 技术在各种业务上采用，有些“恶意”软件伪装成 Web 应用，让传统基于端口的协议识别变得无能为力，如网络游戏、视频、大多数手机应用等。在一些企业和事业单位中，有少数员工通过 IM 应用、社区应用向外散播非法信息，泄露组织重要信息，这些单位面临着较高的法律和经营风险，可能为此蒙受巨大损失。流量增大、应用增多带来的副产物是日志数量变得庞大，有的单位日产生日志量会有几 GB 之多，对周、月的数据统计分析和查询提出了严峻的挑战。如何快速准确的定位和追溯敏感信息的发生、传播和发展是对当前日志系统的重大考验。

1.1 需求痛点

企业单位员工上班时间非法使用邮件、浏览非法网站、网络聊天、在线视频、P2P 下载、炒股的员工日益增加；具体对工作的影响举例如下：

- 办公效率低下，制度形同虚设；
- 网络带宽浪费，网速越来越慢；
- 威胁层出不穷，隐患无处不在；
- 机密信息外泄，业务无形流失；
- 网络违法行为，难逃法律风险；

如何对网络行为进行统计、分析、评估？

如何限制工作时间 IM 聊天、网购、浏览无关网站等非工作行为？

如何封堵 BT、迅雷、优酷等 P2P 行为，并进行流控，提升带宽效率？

如何防范网络潜在的木马、蠕虫和恶意攻击？

如何杜绝通过 Email、网盘等途径潜在的泄密行为？

如何避免恶意发帖、反动言论等法律问题，并在发生问题时有据可查？

1.2 产品特点

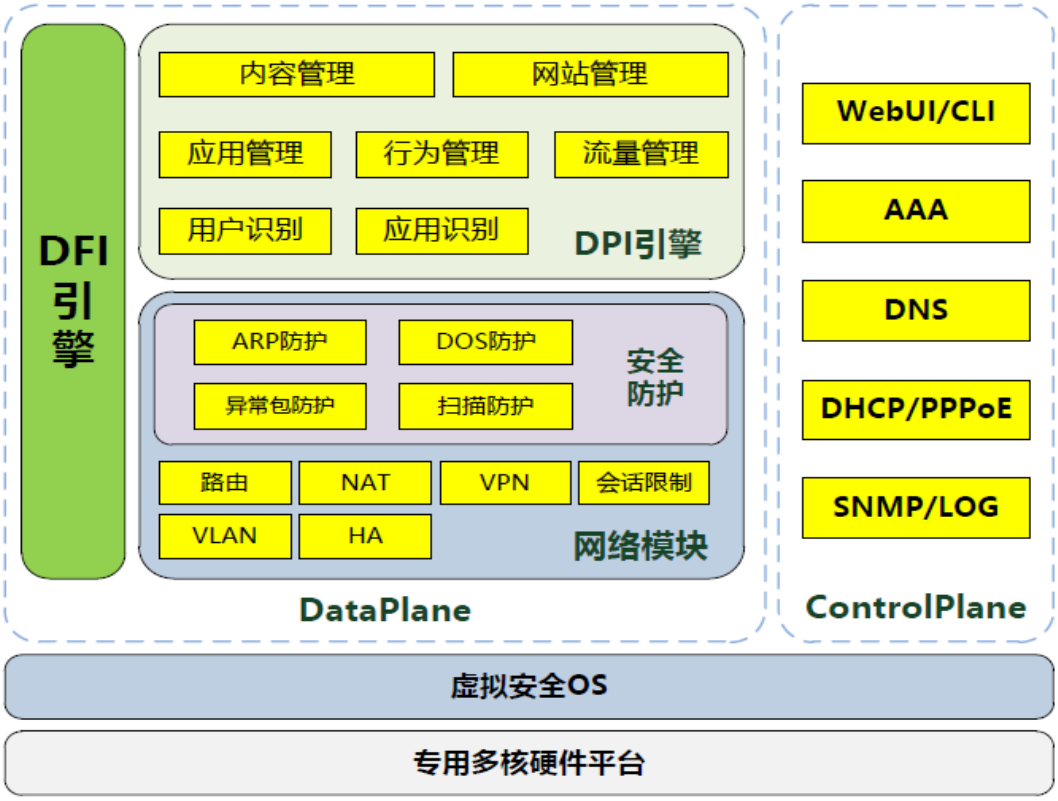
安博通 AG-6000 系列应用网关（以下简称 AG-6000）能对网络中的网络社区、P2P/IM 带宽滥用、网络游戏、炒股、网络多媒体、非法网站访问等行为进行精细化识别和控制。利用智能流控、智能阻断、智能路由等技术，配合创新的社交网络行为管理功能、清晰易管理的日志分析等功能，可以提供业界最全面和完善的上网行为管理解决方案。从而保障网络关键应用和服务的带宽，对网络流量、用户上网行为进行深入分析与全面的审计。

安博通 AG-6000 可对内网用户所有的上网行为进行记录，留存相关日志，支持超过 60 天以上的保存时间，满足公安部 82 号令和无线非经要求；对外发内容关键字进行过滤，规避舆论风险；通过集中管理和数据分析系统可以轻松和网监系统对接，在满足法律合规需求的同时，为用户全面了解网络应用模型和流量趋势，优化其带宽资源，开展各项业务提供有力的支撑。

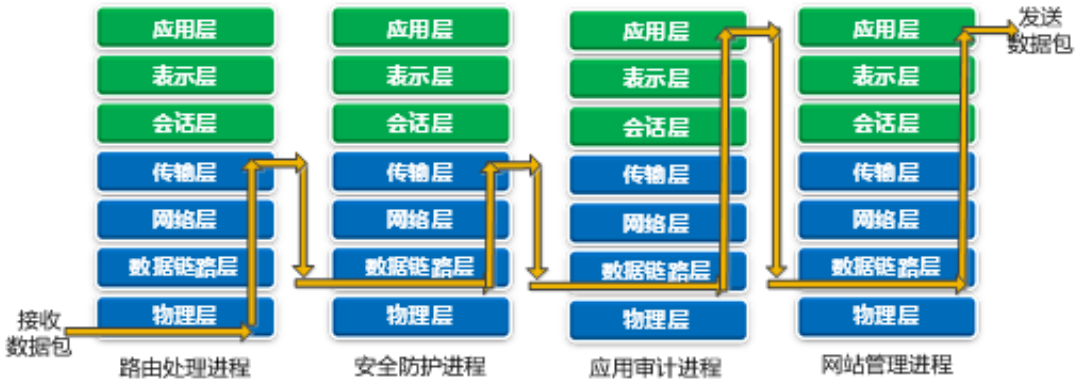
2 技术实现

2.1 高性能多业务并行架构

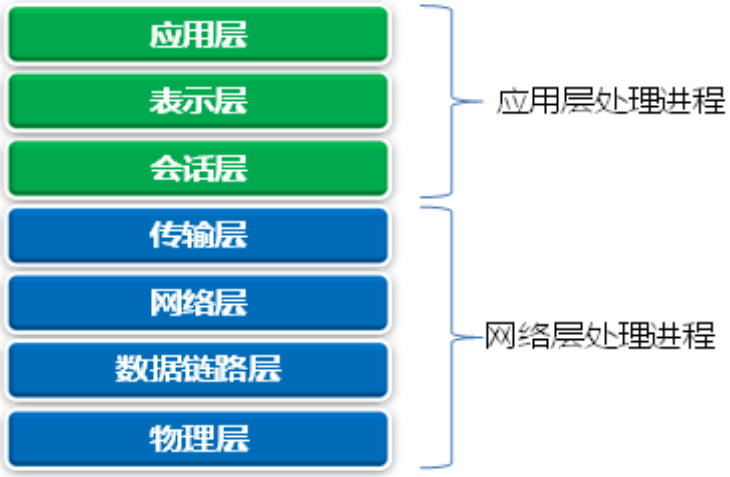
AG-6000 采用最新最先进的多核硬件架构，在硬件架构上运行自主知识产权的安全 OS，高效的并行调度算法和内存管理机制提高了流量转发报文的性能。另外，将 CPU 处理的数据根据其特性分为 Data Plane（数据面）和 Control Plane（控制面）两类，简称 DP 和 CP。在多核系统一部分 CPU 专职 CP 工作，大部分 CPU 专职 DP 工作。这样就避免了因系统调度，导致设备转发性能降级或者无法响应管理操作等现象。具体 DP 和 CP 的 CPU 分布根据用户场景定义。



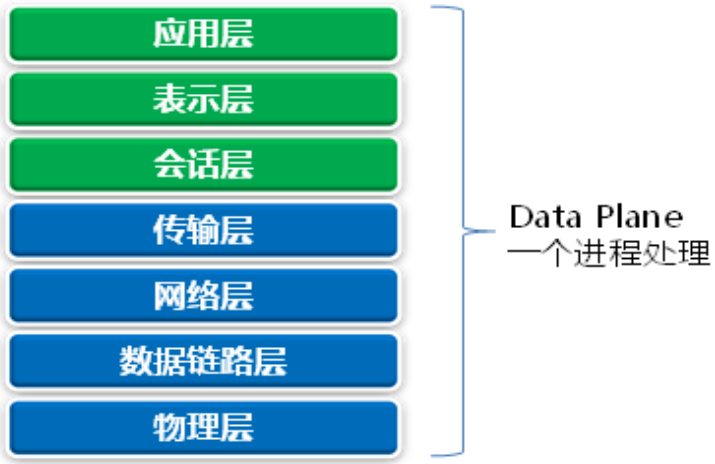
数据面：传统的网关设备为了降低设计和开发难度，会将各个模块以进程的方式存在，数据包每通过一个模块都要重复对数据的解析。增加了数据包在系统停留的时间，从而造成了网络延迟大的问题。



有的设备则将网络层处理与应用处理分别在两个进程上实现，这样就出现了数据包多次拷贝的情况，增加了内存访问次数，降低了系统性能。



AG-6000 系列的 DP 主要处理转发相关的工作，通过对数据包一次解析，按层次由对应模块处理，可以节省不同模块间重复解析数据包所消耗的资源，从而降低网络延迟。



2.2 网络功能特性

2.2.1 多种部署方式

安博通 AG-6000 应用网关可以十分灵活的放置用户的网络中。可以串行接入的方式接入用户网络，部署在防火墙之后，对所有经过 AG-6000 应用网关的数据流量进行分析，实现对应用程序和用户行为的控制，支持路由模式和透明桥接模式；也可以旁路部署的方式，将需要进行审计的网络流量镜像至 AG-6000，可实现对相应的网络流量进行分析，和对上网行为进行统计和记录的功能；同时，AG-6000 应用网关支持混合模式接入用户网络，实现对进入设备的网络流量进行审计和日记记录，对部分的应用数据和用户行为进行审计和控制。

2.2.2 多种路由方式

AG-6000 拥有丰富的路由模式。支持静态路由、策略路由、ISP 路由，RIP、OSPF 等路由功能。

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

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数据应该被转发到一个指定的接口。

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，例如如果网通的服务器通过电信访问，网速就会很慢。AG-6000 安全网关针对该问题，提供 ISP 路由功能，使不同 ISP 流量走专有路由，从而提高网络速度。AG-6000 安全网关提供了四个预定义 ISP 地址库，分别是中国电信（ChinaTelecom）、中国联通（Chinaunicom）、教育网（ChinaEducation）、中国移动（ChinaMobile），同时支持用户自定义 ISP 地址库。之后通过简单便捷的 WEB 配置界面即可实现最优的流量负载均衡功能。

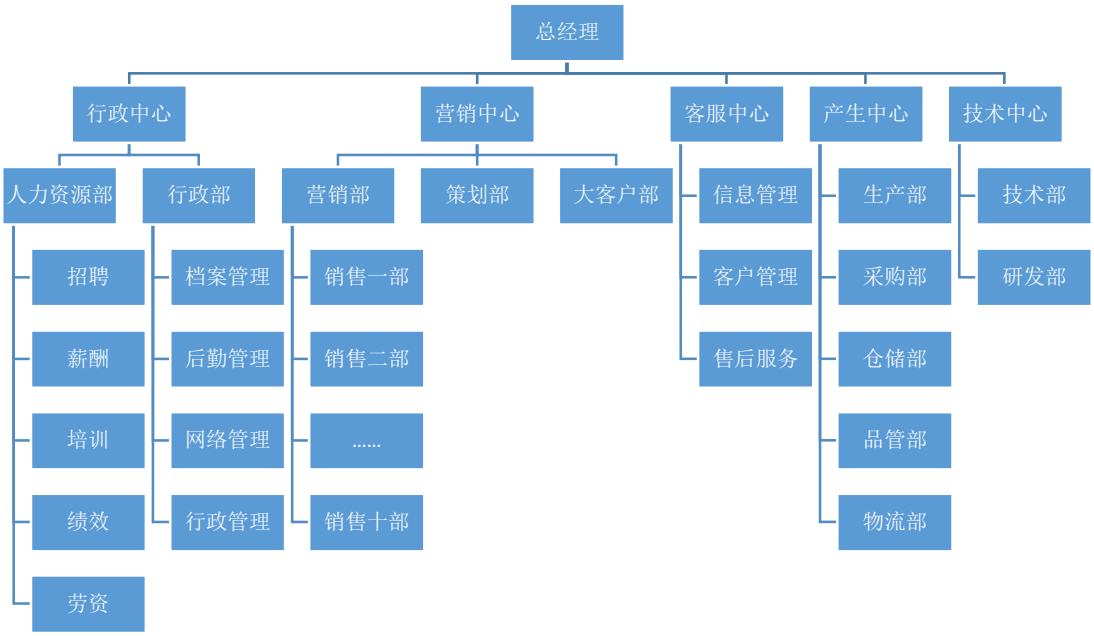
AG-6000 安全网关同时支持常用的 RIP 和 OSPF 这种常用的 IGP 路由协议，可满足用户绝大部分场景下的路由功能的需求。

2.2.3 接口特性

2.2.3.1 多级流量 QoS 管理

AG-6000 系列使用了卓越的应用识别技术，由于该识别技术有效的融合了 DPI 和 DFI 两种识别方法的优点，大幅度提升了应用识别的准确度。但是随着企业规模不断扩大，网络带宽管理需要更精细的管理。对于大多数企业组织架构通常由中心、部门、子部门组成，如下

图：



由上图可知，3 级流控只能满足到基层部门的流控制，对于部门下的应用控制已经明显力不从心，为此 AG-6000 系列提出了 4 级流控，可以满足大中型企业普遍带宽管理需求，策略主要支持基于用户/组、应用/组、服务、源地址等七元组的方式实现带宽管理细化，满足用户各种带宽管理的需求。如下图：

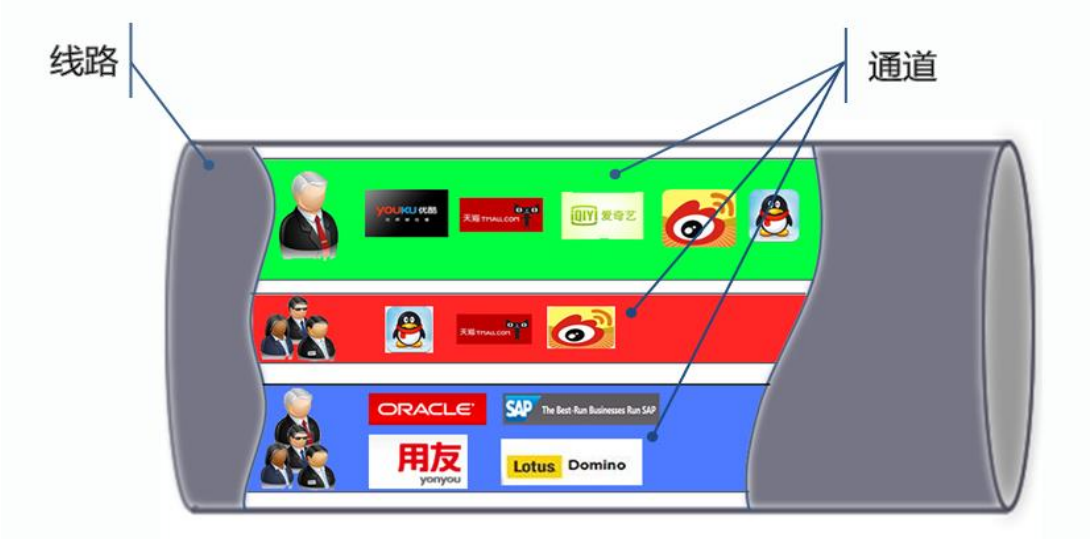
	线路名称	匹配条件					上行(出)			下行(入)			优先级	操作
		源地址	用户	服务	应用	时间	保障带宽	最大带宽	每IP	保障带宽	最大带宽	每IP		
1	某企业	-	-	-	-	-	↑100M	↑100M	-	↓100M	↓100M	-		-
2	营销中心	-	营销中心	-	所有应用	always	↑10M	↑50M	-	↓10M	↓50M	-	高	
3	大客户部	-	大客户部	-	所有应用	always	↑5M	↑20M	-	↓5M	↓20M	-	高	
4	策划部	-	策划部	-	所有应用	always	↑2M	↑20M	-	↓2M	↓20M	-	高	
5	营销部	-	营销部	-	所有应用	always	↑5M	↑40M	-	↓5M	↓40M	-	高	
6	销售一部	-	销售一部	-	所有应用	always	↑2M	↑10M	-	↓2M	↓5M	-	高	
7	P2P限制	-	所有用户	-	迅雷, 迅	always	↑50kb	↑1M	-	↓50kb	↓1M	-	高	
8	邮件保障	-	所有用户	-	广东省教	always	↑2M	↑5M	-	↓2M	↓5M	-	高	
9	默认通道(名	-	-	-	-	always	↑400kb	↑10M	-	↓400kb	↓5M	-	低	
10	销售二部	-	销售二部	-	所有应用	always	↑2M	↑5M	-	↓2M	↓5M	-	高	
11	销售三部	-	销售三部	-	所有应用	always	↑2M	↑5M	-	↓2M	↓5M	-	高	

为了保障业务流转的通畅性、网络使用的正常性，AG-6000 系列在带宽管理方面较传统流控产品来说做了相应提高。

2.2.3.2 引入保障带宽和限制带宽，让业务流转的更通畅

保障带宽：从总带宽中划分出一部分带宽为某种指定流量独享。保障带宽可以保证即使在网络繁忙时，指定流量也能够独占保证带宽。当网络中没有指定流量时，保障带宽部分也能被其他网络流量使用。

下面是带宽管理示意图。绿色通道是 Boss 独享通道，使用应用不受限制；红色通道为员工通道使用非业务应用，该通道对带宽做了最大限制；蓝色通道为业务保障通道，公司的关键业务流量得到保障，其他的通道无法占用该通道的带宽。



2.2.3.3 引入弹性带宽管理，提高带宽利用率

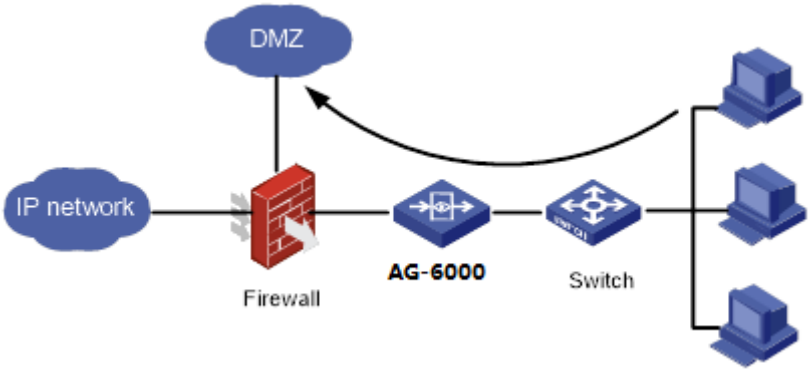
弹性带宽管理，可以使空闲通道不占用大量带宽，减少带宽的浪费，减少因空闲通道占用带宽，流量达到极限出现丢包现象。弹性带宽就是为了解决带宽浪费的问题，空闲通道会自动让出部分带宽给繁忙的通道。一旦空闲通道带宽不足时，将自动抢占回借用出去的带宽。

2.2.3.4 引入自动均分带宽，提升流量的可控性

AG-6000 系列采用了自动均分带宽，当在某个通道中只有一个用户使用时，该用户可以使用全部的带宽，如果有更多用户使用该通道时，带宽将按 IP 数量均分，提升用户上网体验。

2.2.3.5 引入排除策略，避免内网业务被流控

在这个场景下，AG-6000 系列透明的方式部署在防火墙和交换机之间开启流控功能。如果不启用排除策略，PC 终端在访问 DMZ 区的服务器流量会被控制，会影响 PC 终端的正常业务访问带宽，因此需要将这部分流量排除在外，不做带宽控制。



2.2.3.6 链路均衡负载

随着带宽成本的下降及业务需求，企业通常存在两个或两个以上的网络出口，多出口提升了网络出口稳定性同时又带来了多链路带宽利用率低、多链路带宽差异大、各运营商网络质量差异、内网应用对带宽需求差异等问题；以上诸多问题只需通过 AG-6000 提供的链路负载均衡即可迎刃而解。具体实现主要基于以下几点：

- 实时多链路监测：

实时监测每条出口链路的逻辑连通性，即使端口处于 UP 状态，但可能由于远端故障导致的检测报文超时，AG-6000 同样会执行链路切换的动作，以保证网络连接的可用性，实现多条链路的冗余备份。

- 基于权重流量分担：

AG-6000 提供了基于优先级和权重的多链路流量分担算法以满足不同应用场景的需求，从而达到高效的利用出口链路带宽的目的。

- 运营商智能选路：

内置电信、联通、移动和教育网地址库，可以智能的依据目的 IP 运营商属性来决定流量走向，将属于该运营商的访问自动的指向该运营商的链路，实现“南北互通”。

- 智能应用路由：

AG-6000 内置超过 1400 种以上的应用识别能力，将网络中各种应用进行准确分类和精细识别，让不同的应用分别使用不同的出口线路，保证重要业务不中断。

- DNS 透明代理：

通过透明代理技术，完成对客户 dns 流量的无感知代理，从而保证客户的 dns 请求得到最快，最稳定的响应，大幅度提升客户的上网感受。

2.2.4 NAT 特性

AG-6000 拥有优化过的 NAT 性能。支持源地址和目的地址转换，支持动态和静态的地址转换。此外支持 NAT44，可生成和维护用户地址映射表，实现运营商级 NAT 转换；并实现用户溯源关系向 AAA 服务器和日志服务器上报。

相对传统的企业网 NAT 应用，NAT44 具备更高的性能、稳定性和安全性。NAT44 能够支持用户规模更大、承载流量大、业务稳定性要求更高的服务要求。

2.2.5 DDNS

DDNS（Dynamic Domain Name Server）是动态域名服务的缩写。DDNS 是将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析。

目前 ISP 大多提供动态 IP（如拨号上网），若想在网际网络上以自己的网域公布，DDNS 提供了解决方案，它可以自动更新用户每次变化的浮动 IP，然后将其与网域相对应，这样其他上网用户就可以透过网域来交流了

DDNS 可以让用户在自己的或家里架设 WEB\MAIL\FTP 等服务器，而不用花钱去付虚拟主机租金。主机是自己的，空间可根据自己的需求来扩充，维护也比较方便。有了网域与空

间架设网站，FTP 服务器、EMAIL 服务器都不成问题。

如果用户有对 VPN 的需求，有了 DDNS 就可以用普通上网方式方便地建立 Tunnel。透过网域的方式连结，实现远端管理、远端存取、远端打印等功能。

2.2.6 DNS-DNAT

为了规避运营商出口故障带来的网络可用性风险，和解决网络带宽不足带来的网络访问问题，企业往往会租用两个或多个运营商出口。内网用户访问外网的情况下，如果我们通过主机上配置的 DNS 服务器来进行查找，此时返回来的地址并不一定是对应的运营商的地址，访问网络的效果并不能达到理想的效果。AG-6000 系列支持 DNS-DNAT 功能，能让我们对应的链路能够返回对应的服务商提供的服务的地址，解决上网速度慢的问题。

该功能基于负载均衡策略实现，在解决上网速度的问题的同时，也能够解决链路负载不均衡的问题。

2.3 管理特性

2.3.1 设备本地管理

AG-6000 支持 telnet、SSH、WEB 的管理方式。

管理口的默认地址配置为 192.168.1.1/24。默认允许对该接口进行 PING，HTTPS 操作。系统默认的管理员用户为 admin，默认密码为 admin。用户可以使用这个管理员账号从任何可访问设备的地址登录设备，并且使用设备的所有功能。

2.3.2 设备集中管理

可以通过安博通自主研发的集中管理和数据分析平台对 AG-6000 设备进行集中管理,实现集中监控、统一配置下发和提示用户升级并统一升级等功能，同时对网络管理域中的设备上报的安全相关信息收集存储，通过数据发掘提供详尽灵活的统计图、报表，从而辅助管理员进行安全信息审计。利用 DNMS，管理员可以高效地管理各安全网关设备，全面掌握网络的设备情况和整体安全状况。

2.3.3 云平台管理

云平台具有高性能数据运算能力，主要体现在数据的整理和对比 ;具有较大的存储空间，可以保证上传到云端的数据长时间保存。安博通的云管理平台，给用户提供一个云账号，用户就可以根据自己的网络方案述求，将设备统一连到云端，通过云账号统一管理，可以极大的降低用户网络运维的成本。可以让 AG-6000 设备通过云平台实现大规模的设备管理和数据收集整理，根据云端获取的大量数据，去衡量每一个客户的网络是否正常，是否存在隐藏的风险等，宏观地更好地分析客户的网络数据，真正实现一个入口管理整个网络。

2.3.3.1 云端账户管理

可以在云端进行云端账户创建（该用户是超级管理员，可以创建新的用户和用户权限，也可以添加设备），这个超级管理员是可以管理云管理员给他分配的所有资源。同时该超级管理员可以创建管理员，审计员和其他普通管理员。超级管理员可以给普通管理员分配管理权限，给创建的管理员分配可以管理的设备，给审计员分配可以审计的设备，如果没有分配设备，创建的管理员和审计员看不到任何的设备。云端账户的用户权限采用统一分配的方式，基于产品来分配权限。

2.3.3.2 云端设备管理

云端管理通过设备的报活（版本，特征版本，接口，连通性，cpu，内存，流量，连接趋势，用户数，IP 等），可以实现在管理平台上添加设备。可以采用现有网管的方式添加设备，也可以在设备上配置云账户，然后直接将设备添加到对应的用户下（该用户必须是 admin 用户）。所有的设备按照一定的原则，树形结构呈现。每一个超级管理员，可以看到他所管理的全部设备，超级管理员创建的普通管理员，只能看到超级管理员给其分配的管理设备。拥有这些设备权限的用户，可以看到这些设备在全球的分布情况，通过报活的 IP 地址查询。

2.3.3.3 云端管理设备的功能

设备连接云端之后，云端根据安博通公司版本发布情况，定期提示设备完成升级，可以从云端下载升级包，也可以通知设备，在特定的时间，从特定的地址下载升级包。然后根据下发的升级任务，定时的在设备端完成自动升级，从而保证全网接入云端的设备，版本跨越度不超出 3 个版本。可以根据管理员自定的设备组，然后依据我司版本发布情况，定时的通知管理员，设备需要升级，目前系统最新版本是****。

升级内容除了上面提到的版本升级之后，还有设备端相关特征库的升级，升级方式和版本升级完全一致。

云不仅提供设备升级相关的功能，还需要提供一定的管理设备，统一下发策略的功能，主要包含：ACL 策略，流控策略，VPN 策略等策略形式相关的功能。这类性的功能主要是统一下发形式。管理员选定下发的设备组，然后策略就可以统一下发，或人为下发等。

除了统一下发管理功能外，云端需要支持设备的反向管理功能，每一台连到云端的设备，不管该设备部署在内网，还是部署在互联网，通过云端都可以反向登录设备。保证云端管理员可以特定的操作每一台设备。前期交付设备的界面反向登录即可

云端提供集中认证的功能，管理员可以指定设备组，使用云端的相关认证。保证认证的统一管理，统一部署。

2.3.4 用户管理

用户管理模块作为行为管理设备和防火墙必不可少的模块，使用频道在大幅提高，已经从初期的有无，是否可用，到用户作为系统的一个重要资源，在安全策略、认证等功能上都会相应使用。

AG-6000 系统的用户类型有：第三方用户，未定义用户和属性组用户，可以实现基于用户的搜索，支持用户的移动、修改、导出、导入和批处理等功能。提供基于 IP、MAC 和 IP&MAC 的用户识别方式。用户支持设备上的 AD 导入和厂商自定义导入功能。外部导入的用户全部在第三方用户组中显示。这部分用户在和服务器断开连接之后，可以将用户移动到根目录下，但是在未和服务器断开之前不能移动。

AG-6000 支持全面的用户属性字段，如：姓名；显示名；英文名；英文缩写；办公室；电子邮件；电话；手机；部门；职务；公司；备注；年龄，使用的终端等各种属性等客户可能使用到的所有属性，满足用户需要根据用户的某一种或者多种属性筛选出对应用户的需求，方便在策略中引用。具体支持情况以当前发布版本为主。

2.3.5 用户组管理

大多数设备中的组都是普通的用户组织结构组，从功能定义角度看，一个用户只能属于一个普通组。但是在实际使用的场景中需要把一堆不在一个普通组下的用户放到一个虚拟组。AG-6000 设备端提出了权限组和属性组的概念，两个组最大的区别是普通组的用户没有先后顺序，而权限组中的用户，只能通过创建和修改用户组的时候直接编辑选择那些用户放到这个组下面。

属性组创建的时候只要选择属性组所关心的普通组的组织目录结构，然后选择一个或多个用户的相关属性，点击创建，设备就会自动的将这个普通组目录下包含这些用户属性的用户添加到这个组中。后期创建的用户，只要有符合这个属性的，也会自动的添加到这个属性组中，方便策略使用。

AG-6000 支持用户组的创建、移动、搜索等功能。用户组织结构通过优化结构呈现，默认展示一级用户组目录。用户鼠标点击一级目录，则从后台获取一级目录下对应的二级目录展示，同时在页面的右半部分展示用户点击的一级目录下的用户和用户组。

2.3.6 应用识别

应用识别（Application identify)是 AG-6000 系列的重要功能。借助于应用识别功能，可以准确识别网络上正在运行的应用，应用流量的准确识别不但可洞悉整个网络的运行情况，而且可针对具体需求做用户行为的准确管控，这在一定程度上既可保证业务流的高效运行也可预防由于内网机器受到攻击而生产的威胁，同时识别应用类型也是应用审计与应用流量控制的基础。

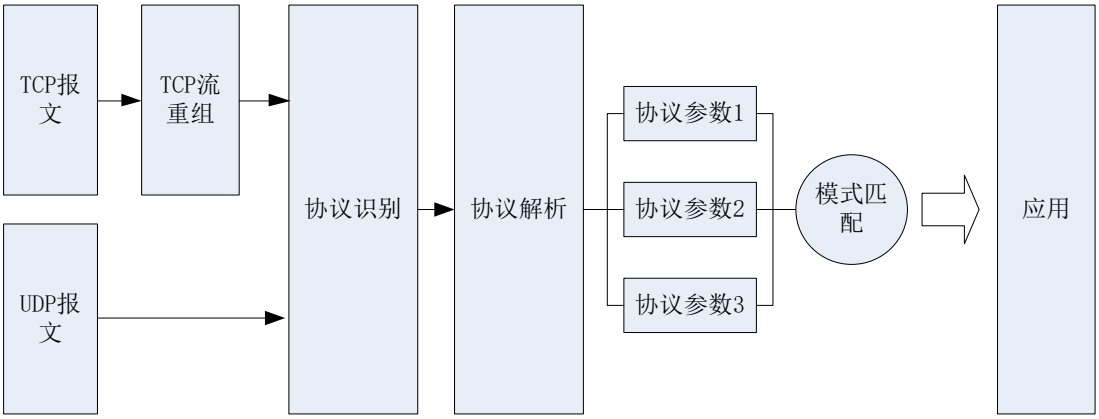
随着 P2P 应用的广泛流行和基于 Web 的应用的兴起，令传统的利用固定端口来区分应用类型的设备无能无力。应用识别功能把对报文的协议解析、深度内容检测以及关联分析结合起来，通过对大量实际环境中的流量的分析，总结出每种应用的流量模型，把对数据包的协议解析、深度内容检测和关系分析的结果综合起来，由决策引擎通过与流量模拟的匹配程度，智能的判定应用类型，相比传统的应用识别技术，还具有以下特点：

2.3.6.1 基于协议状态分析

AG-6000 系列对已知协议和 RFC 规范的深入理解，可准确、高效的对各种协议进行解

析。例如，对于一次 HTTP 访问，先由协议解析出访问的 URL、Host、User-Agent 等信息，再将解析出来的信息进行特征匹配，这样可以带来以下优点：

- 提高性能，不需要对整个报文进行模板匹配，可以提高应用识别的性能。
- 降低误识别率，因为进行模式匹配的字段由整个报文缩小为特定的协议参数，可使特征写的更加精确，减少误识别率。



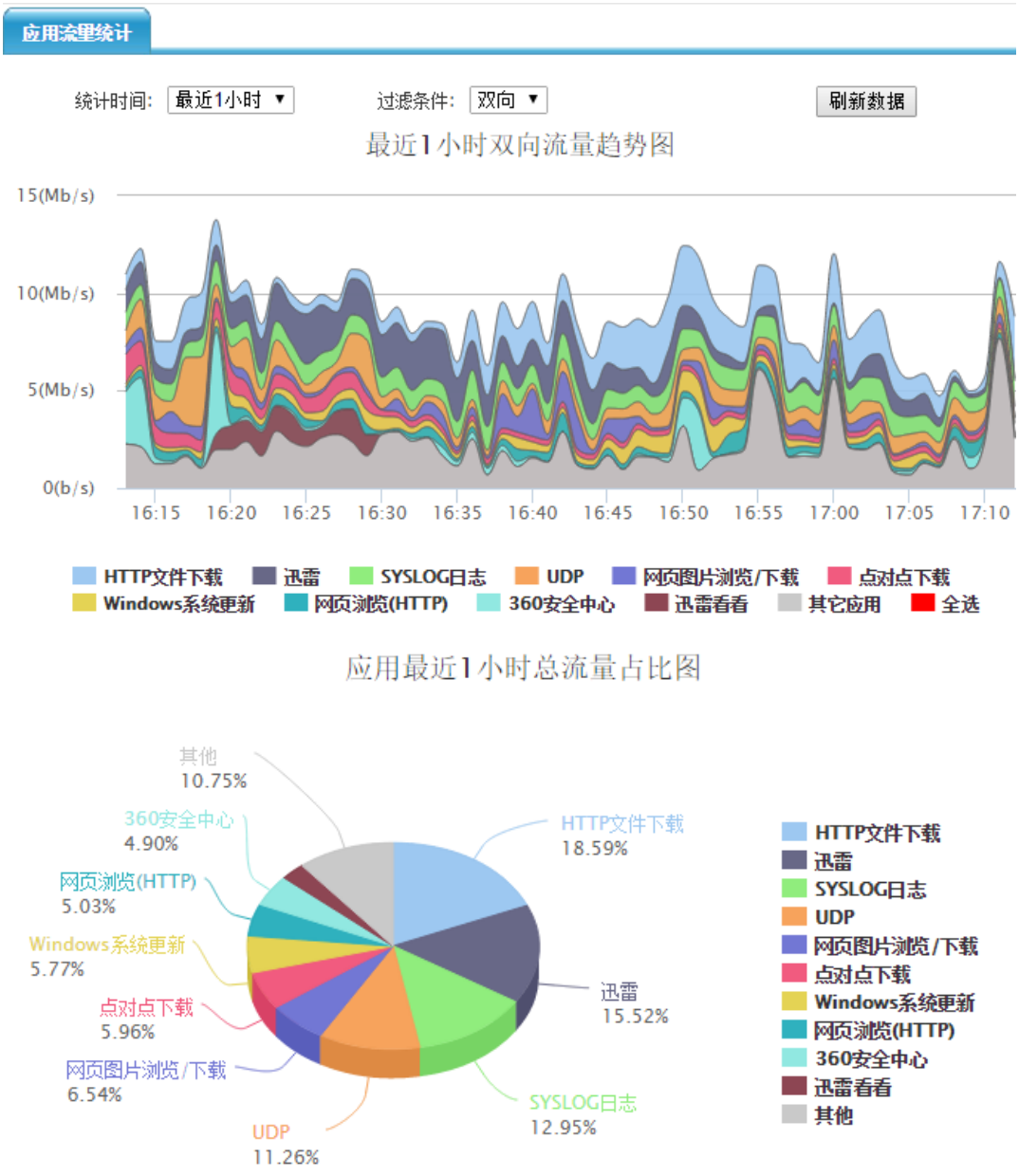
2.3.6.2 行为检测

不同的应用类型体现在会话连接或数据流上的状态各有不同 ;基于这一系列流量的行为特征，通过分析会话连接流的包长、连接速率、发送/接收的流量比例、包与包之间的间隔等信息来识别应用类型。

只有在准确识别应用协议的基础上，才能对应用做到深入、全面和准确地控制。不但可以准确、高效的识别出网络流量的应用类型，而且可以精准的识别出应用的行为。随着特征库的不断更新，支持的应用和行为在不断增加。网络中的应用日新月益，拥有强大的安全服务团队的支持，可以随时对网络中的新应用进行跟踪分析，持续的更新应用特征库。

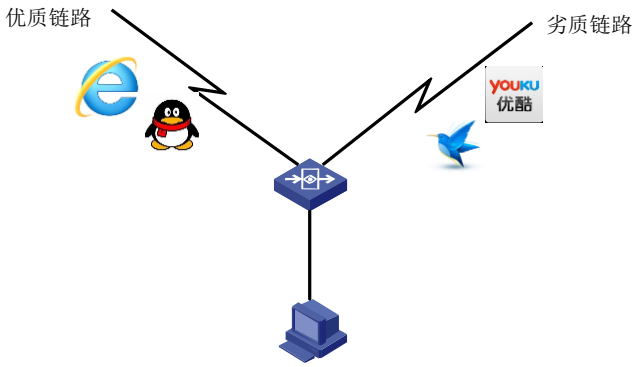
2.3.6.3 应用流量统计

借助于强大的应用识别，用户可以通过应用流量统计查看到网络中的应用流量组成，准确了解网络的使用情况。



2.3.6.4 应用路由

AG-6000 系列通过配置策略路由，可以实现基于应用的路由选择。在用户有多条链路的情况下，不同的应用分别使用不同的线路，使办公、游戏等重要应用的流量使用链路状态较好的线路，使 P2P、视频等流量走链路状态较差的线路，帮助用户合理的分配链路资源，即保证重要业务的使用，也不影响 P2P、视频等的使用。



AG- 6000 系列的应用路由功能是不是基于端口，而基于应用来实现的，当发现某种应用的流量的时候，会把对应的 IP + 端口信息缓存在系统中，相同的 IP + 端口再次新建会话的会话，会命中相应的缓存，从而实现应用路由的功能。

2.3.6.5 基于应用的流量管理

AG-6000 系列可以实现基于应用的带宽分配，帮忙用户更好的限制 P2P、视频等占用带宽比较高的业务，保障重要业务的运行。

2.3.7 应用策略

应用策略分类两大类：应用审计和 URL 审计。

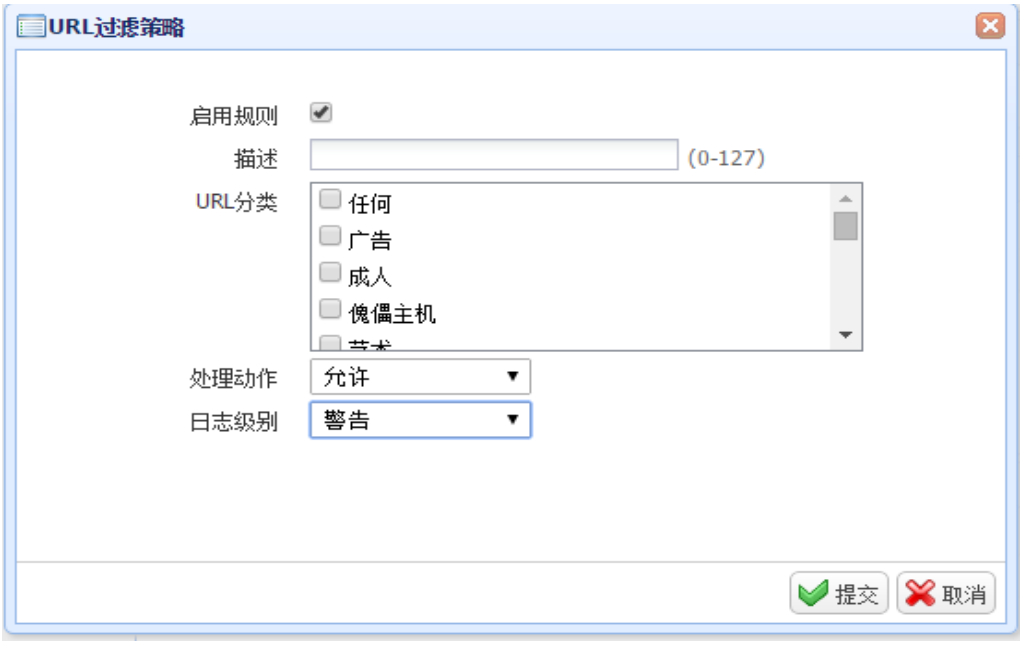
2.3.7.1 应用审计

应用审计，是通过对数据包的深入解析，获取应用的行为及操作内容。通过用户配置的关键字进行匹配。达到对互联网访问的行为控制和内容控制的目的。其依附于安全策略，减少了数据包的过滤范围，并有针对性（针对用户、应用）的进行审计和记录。

应用审计是基于应用+行为+动作+关键字的四维匹配条件，可以实现精细化的控制。可以实现允许查看微博，但是不允许发送精细化控制。

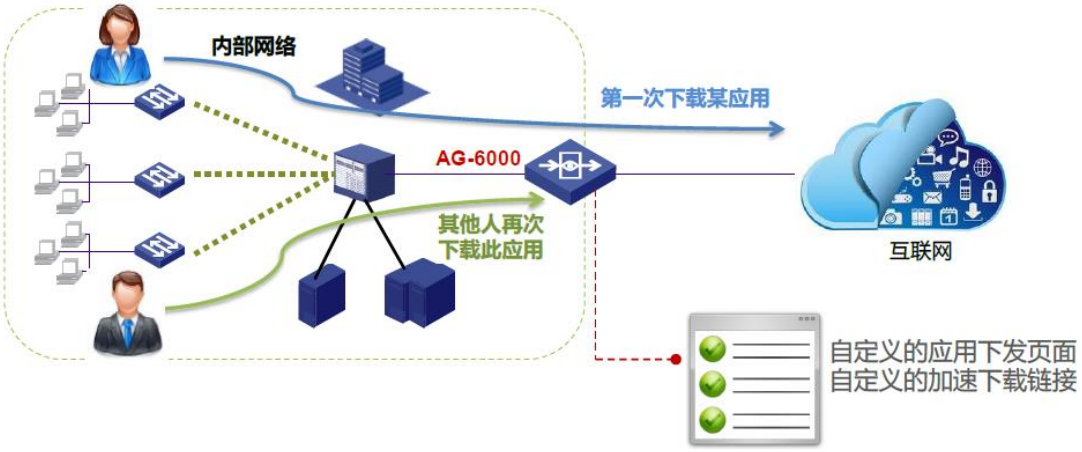
2.3.7.2 URL 审计

URL 策略，是通过 URL 分类库，对网站访问进行过滤。让用户通过网站分类的选择，轻松控制网站访问。同样，URL 过滤也依附于安全策略。可以减少了数据包的过滤范围，并记录访问网站及 URL。



2.3.8 APP 缓存应用快速下发

AG-6000 创新的将 APP 缓存在设备本地，当用户下载时直接推送，几十 M 的文件只要几秒钟，极大的提升了带宽利用率的同时大大加速和提升了用户体验；并且支持 iOS 和安卓 APP 的缓存，业界技术领先；在低成本的投入下同时为客户的终端营销推广开辟了新的方向。



2.4 访问控制和审计

现代的网络应用发展已经从以前单一的功能，向着多功能的方向发展。比如 QQ，以前只是作为一种通信工具，传输消息，现在 QQ 可以传文件、发微博、购物、发邮件等等；丰富的应用功能让企业管理者对内部资料泄密和员工工作效率下降大伤脑筋。AG-6000 系列提供以访问控制、事后审计、用户轨迹三大功能。核心思想是帮助 IT 管理员使整个网络易用、安全。IT 管理员可以从用户、设备、应用、行为等多个视角来管理分析网络。

2.4.1 丰富的身份认证手段

有效的区分用户，是部署差异化授权和审计策略、有效防御身份冒充、权限扩散与滥用等的管理基础；并且安博通以用户需求为导向，领先的实现了用户急需的微信认证。

AG-6000 的身份认证方式有：

- 本地认证：Web 认证、用户名/密码认证、IP/MAC/IP-MAC 绑定；
- 第三方认证：RADIUS、LDAP 等
- 短信认证：传统的认证方式，方便快捷；
- APP 认证：不需要借助数据中心软件，无需 APP 修改，避免协调沟通成本；
- 微信认证：连接商家 WIFI，自动弹出“一键微信连 WIFI”并关注微信公众号；

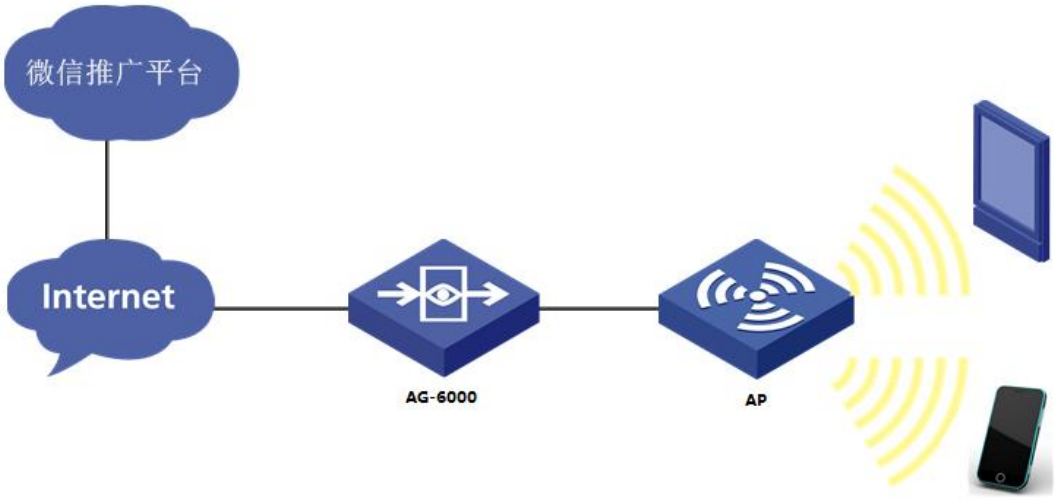
2.4.1.1 一键微信认证

微信认证作为国内最知名的手机移动应用之一，已经得到了大量普及。虽然原始认证的方法短信认证和本地密码认证可以解决动态认证问题的，但是繁琐的操作或者短信费用几乎成为了大众的噩梦。因此，微信认证应运而生，即解决了动态认证的问题，又减少了认证操作的步骤，且没有额外的资费，还帮助商家推广微信公众账号。

微信采用双 ID 实名审计和商业推广两面大旗，即微信 ID 和 openId。微信 ID 用来标识用户唯一性。openId 是微信 ID 与公众号 ID 共同产生的唯一标识。在公众平台只认 openId 不认微信 ID，有了 openId 和 AG 微信认证平台结合，对于同一个公众号就能根据微信用户所在的不同地点，推送不同的推广信息，辅助客户完成精准广告推送。为了简化用户的认证

过程，二次到店支持免认证，直接关联上 SSID 即可自动认证通过并上网，用户无感知；给用户超预期的体验，提高企业品牌认可度。

拓扑示意图：



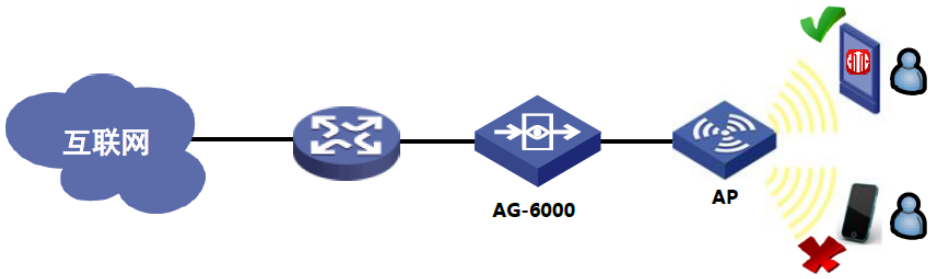
一键认证步骤：

- 连接商家的 WIFI；
- 弹出微信认证界面；
- 点击“一键打开微信连 Wi-Fi”;
- 点击“立即连接”即可通过认证。

2.4.1.2 APP 认证

大型超市、连锁门店、4s 店等商贸连锁企业，纷纷业推出自己 APP，紧跟 e-commerce、O2O 时代步伐，用于丰富自己业务线、推广营销、会员返利活动。然而 APP 如何进行高性价比推广，为此 APP 认证孕育而生。

APP 认证首先需要管理员在 AG-6000 预定义配置 APP 特征，网关会根据此 APP 特征生成符合设备可识别的特征文件加入到特征库中， 当移动终端连接上 WIFI 后并打开相应的 APP 触发网络流量，AG-6000 自动识别流量并进行特征匹配，即可判断连接上的移动终端是否合法。



2.4.2 精细化的访问控制

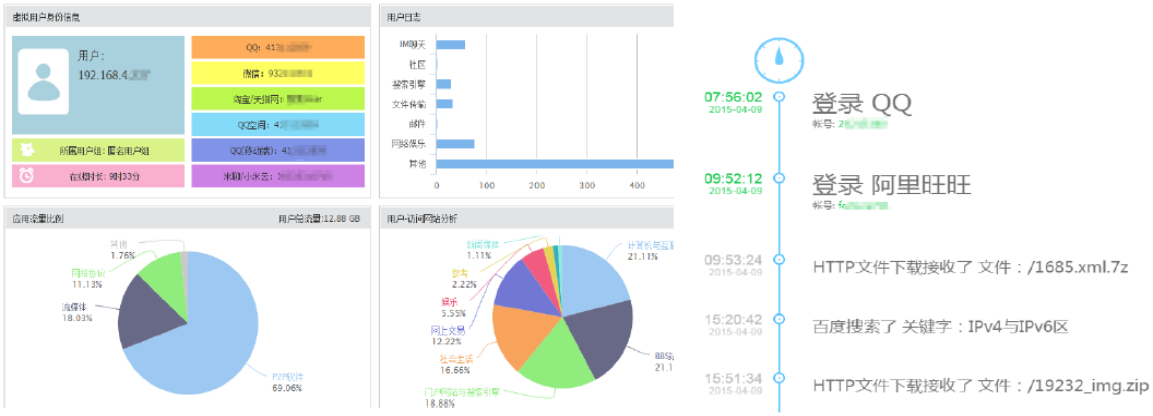
随着 WEB2.0 技术的蓬勃发展和动态端口的新应用层出不穷，使得传统网关产品采用五元组的访问控制方式早已变得力不从心，而 AG-6000 的出现让访问控制变得简单，基于 7 元组以及时间的访问控制策略，能有效的控制自然人、应用的访问控制。在该访问策略中，还可以对应用行为和内容进行控制，比如控制 QQ 传文件但不控制 QQ 收发消息；过滤关键字，防止涉密信息通过邮件泄密等等。

2.4.3 防止私接路由

可应用在跨三层的网络环境，能够快速识别“一拖 N”的网络私接行为，精准定位“N”即私接用户数量，并进行有效的管控；及时发现非法热点预防个人用户私接路由，拒绝未知网络终端节点，保护运营商利益；让整个网络拓扑清晰可控，有效预防数据泄露的安全风险；极大的降低了管理员网络维护的工作量。

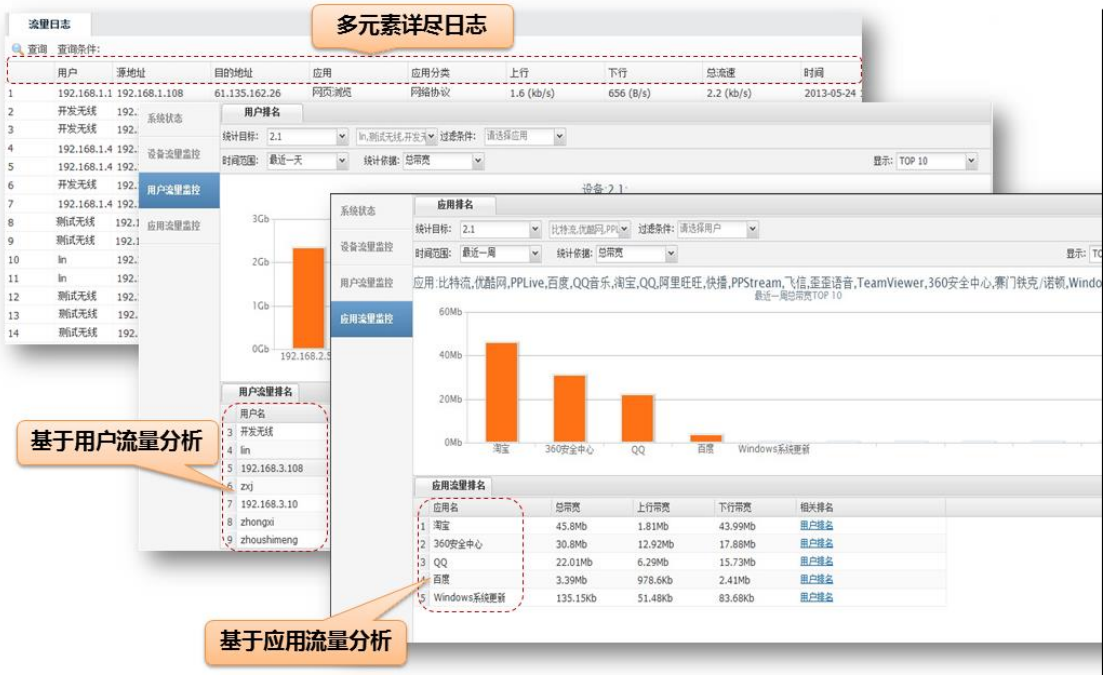
2.4.4 基于用户的行为轨迹分析

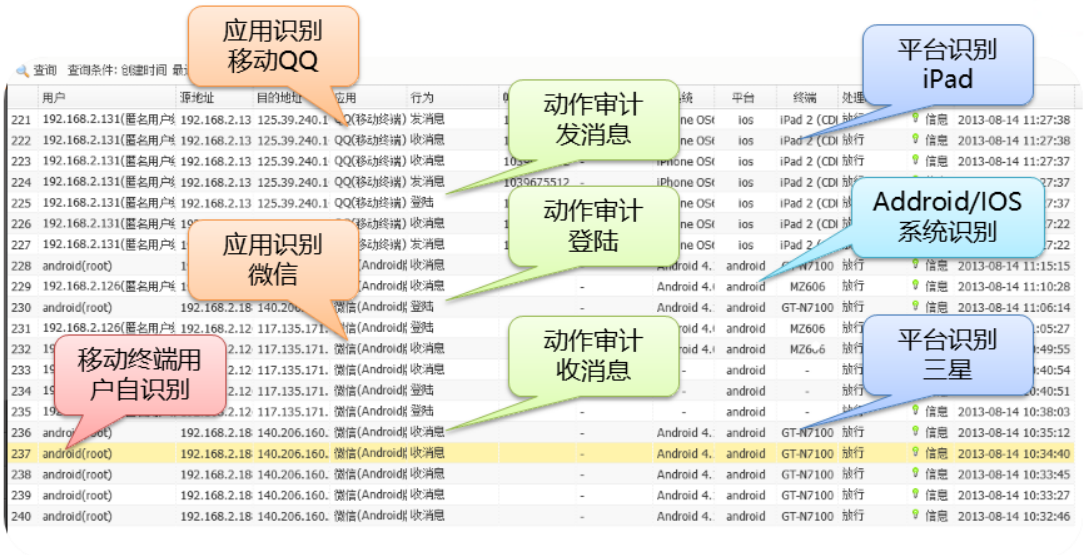
通过搜索引擎的方式对用户网络账号、行为动作、虚拟账号、关键字分析及上网时长等多维度的用户信息进行关联数据分析，真正实现了基于用户的上网行为管理与审计的可视化，将用户的上网行为轨迹清晰直观的加以呈现，有助于网络管理人员制定更有针对性的网络管理策略，保障网络资源的合理有效利用和工作效率提升。



2.4.5 清晰的事后审计

AG-6000 系列产品支持详细、清晰、易用的日志特性，可以全面记录审计用户上网行为、使用流量、访问网站、所用终端系统及设备类型平台等信息；日志支持定制化过滤器，可根据 IP 地址、认证用户、访问应用、访问 URL、发帖内容等要素进行搜索，让事后审计省时省力,可支持对 HTTPS、邮箱类解密策略的配置。同时，AG-6000 产品提供丰富美观的报表，以柱状图、饼状图、百分比等形式最直观地体现网络运行状况，让网络管理规划有据可循、有的放矢。





2.4.6 SSL 网站解密

互联网时代，越来越多的网站启用 HTTPS，而随之而来的是员工利用这种加密方式泄露企业敏感信息的可能性也越来越大；并且由于 HTTPS 网页经过了加密，采用普通的流量分析方式是无法审计到访问行为的，那么就意味着员工使用 HTTPS 的方式进行娱乐，企业是无法清晰准确的了解员工的工作状态和网络的运行状态。为了保障企业有清晰的事后审计，保护企业机密，AG-6000 系列提供了 HTTPS 审计功能，AG-6000 系列采用特有的加密流量识别技术，能够对主流的加密网站、加密网站搜索记录、加密邮件等进行行为识别。管理员可以采用自定义的方式，定向审计用户和加密网站，让网络运行情况更加清晰明了，做到管理规划有据可循、有的放矢。

2.4.6.1 工作原理

解析 DNS 报文，设备获取 DNS 回应报文，匹配解密策略的源地址组，解析出域名对应的 IP，往当前策略上添加 IP 域名信息。

转发报文流经设备，判断 TCP 443、995、993、465 端口进入解密策略匹配流程。依次匹配入接口、源地址对象、目的地址对象、若为 443 端口判断目的 IP 是否存在于 DNS 解析的 IP 中，若均匹配上报文送入 linux 内核，通过内核的 iptables redirect 功能重定向到本机代理进程。

代理进程建立双向 SSL 连接，并对数据进行加解密，解密后的数据封装 SKB 后送入审计流程。

2.4.6.2 解密策略

解密功能通过策略的方式检查哪些流量需要进入解密流程，匹配流程放在报文转发流程中，不需要对本机报文进行解密。

https 解密策略从四个维度判断是否处理当前报文：入接口、源地址、目的地址。域名

IP。

邮箱类解密策略从三个角度判断是否处理当前报文：入接口、源地址、目的地址。

网页版邮箱需匹配第四个维度-域名，该域名系统内置。

注：源地址、目的地址、域名均以地址对象的形式配置。https 解密策略支持例外域名配置。

2.4.6.3 数据解密

https 站点解密，系统内置的站点支持 https 解密功能，目前系统提供 128 个常见的站点域名，并且客户可以根据自己的需要自定义 10 个域名。使用设备自带的证书签发功能，或支持导入第三方证书，并被解密策略引用生效。用户证书一旦被解密策略引用，在证书过期之前，策略中包含的其他域名即可顺利的完成浏览。

解密功能提供特定站点排除功能以及源地址排除的功能，针对排除的地址和站点不做 https 的解密，两者之间是或的关系，只要一个满足即排除不做解密，源地址排除功能使用地址对象配置。

系统自带的站点格式举例：

www.baidu.com

www.taobao.com

www.jd.com

www.sogou.com

www.so.com

www.taobao.com

www.amazon.cn

注：所有系统自带，自定义的，不支持涉及金融类的&&交易类 https 网站解密。

加密邮箱解密，该功能目前只针对如下常见邮箱提供解密：QQ（个人，企业），网易（163/126），标准的 pop3（995）、imap（992）和 smtp（465）同时开启 ssl 加密的邮箱。

2.4.6.4 证书管理

设备自身支持证书签发的能力，可以为 IPsec VPN，https 解密等功能签发相关证书。

支持证书导入导出的功能，方便证书的管理，并且可导入第三方证书。解密策略在用户证书中选取一个证书使用，且支持证书之间的切换，证书被其他模块引用时仍可被解密策略引用。

2.5 终端识别和审计

AG-6000 提供以终端识别引擎为核心的安全策略、行为审计、来宾访问、日志分析四大功能。核心思想是帮助 IT 管理员使整个网络易用、安全。IT 管理员可以从用户、设备、应用、行为等多个视角来管理网络。

2.5.1 终端识别

终端识别引擎是主要提供用户身份验证、和终端、系统类型识别的功能。当员工携带自

己的设备连接到公司的网络之后，不需要安装任何客户端，只需要打开浏览器，就可以轻松的完成用户身份认证，并获得相应的授权，这样不仅可以减少 IT 管理员的负担，最重要的是，简化了操作，提高了员工使用自带设备的积极性。在不安装任何客户端软件的情况下，通过身份识别引擎的设备分析模块，IT 管理员可以看到员工加入的网络中的设备的操作系统、硬件类型和生产厂商。

AG-6000 识别用户系统、终端的方式有两种：通过 Web 访问的 User-Agent 域来识别终端类型。

```
GET / HTTP/1.1
Host: m.baidu.com
User-Agent: Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_3_3 like Mac OS X; zh-cn)
AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8J2 Safari/
6533.18.5
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
Cookie: Hm_lvt_e8499b7329e8d5d44f3f4c8902bb043a=1372659521;
```

通过移动应用来识别。比如在应用的流量中发现了来自淘宝网(IOS)客户端的流量，那么会通过这些流量判断用户的设备类型为 iOS。

2.5.2 安全策略

IT 管理员可能针对不同的场景，针对特殊的人员和设备类型，灵活的制定安全策略，一般来说，对于访客，对设备类型做比较少的限制，同时给只给予少量的权限，对于公司的管理人员，在给予更多权限的基础上，还要对设备类型做出更严格的控制，下面给出一些例子：

安全级别	人员	设备类型	权限
低	访客	任意设备	Internet
中	员工	iPhone	Internet、公司邮箱
高	经理	iPad	OA系统

2.5.3 来宾访问

当有访客携带自己的智能手机/平板电脑尝试加入到公司网络中，这些访客可以使用来宾访问的功能。

- 不需要通过复杂的验证，不用安装客户端，就可以正常的连续到网络中
- 受限的访问控制，确保公司内部资料不会被泄露。
- 支持上网行为审计，如有需要，可以对来宾开启网络行为控制。

2.5.4 日志分析

所有的系统日志中都会记录有系统、终端类型。这些信息可以有效的帮助 IT 管理员评

估网络状况。

2.5.5 支持的设备列表

AG-6000 的终端识别和审计适用于市场上主流的设备 :Windows、iPhone、iPad、Android 等。

2.6 互联网出口特性

总分结构组网下，为保证业务质量客户经常会使用多线路接入，例如使用电信、网通等两条以上互联网出口链路，那么如何同时复用多条链路并做到流量的负载均衡与智能分担

AG-6000 集成链路负载均衡、ISP 路由、策略路由等多种互联网出口特性。

2.6.1 链路负载均衡

根据动态算法，AG-6000 能够在多条链路中进行负载，算法配置简单且具有自适应能力。可通过带宽比、优先级等多种方式设置负载策略。针对不同接口可设置阈值，当达到阈值后可不再进行负载流量。同时可调用健康检查策略，检查每个负载均衡接口的联通状况，监控业务状态。

2.6.2 服务器负载均衡

服务器负载均衡（后简称“SLB”）就是对一组服务器提供负载均衡业务，这一组服务器一般来说都是处于同一个局域网中，并同时对外提供一组或者多组相同或相似的服务。

SLB 包括以下几个基本元素：

- 集群（cluster）:对外提供特定服务的服务器群体，包括负载均衡设备（LB product）和 server；
- 负载均衡设备（LB product）：负责分发各种服务请求到多个 server 的设备；
- Server：负责响应和处理各种服务请求的服务器；
- VS IP：对外提供的虚拟 IP，亦即公网 IP，供用户请求服务时使用；
- Server IP：服务器的 IP 地址，供负载均衡设备分发服务请求时使用；

2.6.2.1 工作原理

AG-6000 系列 SLB 实现方式的原理如下：

用户请求 cluster 前端的负载均衡设备的 VS IP，此时负载均衡设备上的虚服务接受用户请求，依次根据持续性功能、调度算法、选择真实的服务器，然后再通过地址转换，用真实的 server IP 地址替换 VS IP，最终将用户的服务请求转发给各个真实的服务器，服务器处理完服务请求，将响应报文回复给用户，当响应报文通过负载均衡设备时，报文的源地址会被还原为 VS IP 地址，然后负载均衡设备再将响应报文返回给用户，完成整个负载调度过程。

2.6.2.2 基于权重负载均衡算法

实服务组 S 下面有多个 dant 规则 A、B、C，且均为 active，分别为其配置权重为 Wa、Wb、Wc，则总权重为 W=Wa+Wb+Wc，产生一个随机数 R，对总权重取余 val = R % W，确定 val 所在的范围，最终选择实服务器，即 DNAT 规则。适用于服务器集群中各个服务器存在差异的情况。

基于源地址散列+权重算法: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，基本算法同加权随机算法一致，这里用源地址的 hash 值 H 代替上面的随机数 val = H % W，确定 val 所在的范围，最终选择实服务器，即 DNAT 规则。适用于服务器集群中各个服务器存在差异且需要同一用户的报文发往同一服务器处理的情况。

2.6.3 ISP 路由

AG-6000 提供 ISP 路由功能，多出口场景下，用户业务通过不同运营商的线路，链路质量会有下降，出现网络访问缓慢等问题，AG-6000 预置 ISP 地址库，分别为中国电信（ChinaTelecom）、中国联通（Chinaunicom）、教育网（ChinaEducation）、中国移动（ChinaMobile）四个主流运营商，并可自定义 ISP 地址库，针对明确运营商线路的应用，指定运营商线路，从而使得业务质量最优。

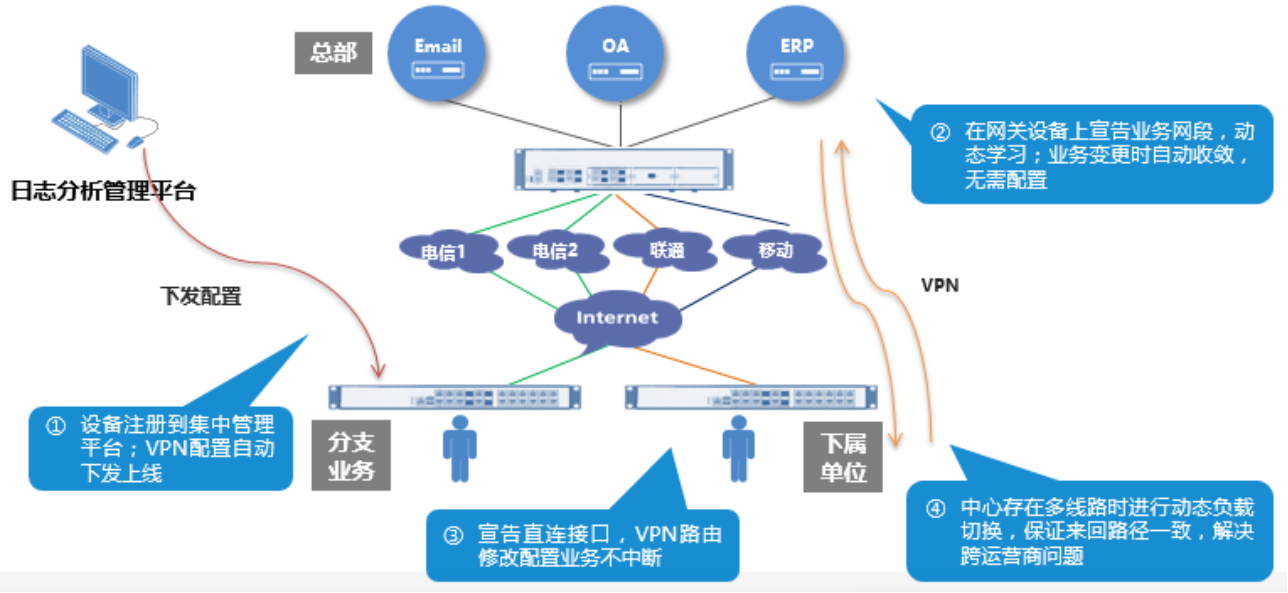
2.6.4 策略路由

AG-6000 支持策略路由功能，传统的路由策略只能指定 IP 包下一跳转发地址，AG-6000 策略路由，不只是简单的跟进目的或者源 IP 地址来决定，通过接口、地址、用户、应用、服务等 7 元组策略，控制 IP 包转发流向，从而在互联网出口的场景下，更契合场景，更加灵活。

2.7 快易IPsec VPN

AG-6000 的 IPsec VPN 模块具有业界领先技术，在复杂网络环境下大大简化了管理员的维护工作量，配合集中管理和日志分析平台，可实现 IPsec VPN 快速零配置上线。快速对接模块式下，隧道接口感兴趣流等可无需配置自动协商，整个 IPsec VPN 网络全自动收敛，自适应多线路，完美的解决了分支运维能力弱的问题。而独创的主备切换 0 丢包技术，可实现 TCP 业务不中断，完美的解决 HA 切换业务中断的问题，可让管理员高枕无忧。

对金融、能源、交通等行业一些分散型的营业网点，对于业务连续性以及内网数据安全要求非常高。在租用运营商的固网光纤专线作为主链路的同时，还需一条安全稳定的备份链路以应对突发状况，专线成本高、灵活性差的缺点暴露无遗；AG-6000 支持 3G/4G 网络并支持 3G/4G IPsec VPN 加密连接进行链路备份。连接提供按需拨号，无需改变原有网络架构，在主线路故障时主动承接和中心端的网络加密通信，具备数据完整性、数据传输安全、高性价比、网络无改变等特性。



2.8 无线非经合规

国家 GAWA3011.(1~5)-2015 公共场所无线上网安全管理系统无线上网接入要求规范，如咖啡馆、酒吧、KTV 等提供网络接入的公共场所，需实现规范的准入管理制度，上传审计信息到网监后端平台，否则会面临业务下线、停业整改、罚款等风险。

AG-6000 提供无线非经合规特性。并可适用于集中式部署、分布式部署、旁路对接多种场景，从而易于客户网络平滑升级。公安部提出了标准要求，但各地市的对接标准不一，后端对接厂商众多，也给客户带来了升级困扰。AG-6000 支持任子行、派博、洪旭、爱思、博网等多家主流后端对接厂商平台，对接地区广，对接经验丰富。有在银行、运营商、零售连锁等多种场景丰富的对接经验，超高的应用识别率、定制开发能力，为客户场景的安全合规提供保障。

2.9 集中管理和数据分析系统

安博通集中管理和数据分析系统是提供对 AG-6000 的集中监控、配置和升级，并且对上报的安全相关信息收集存储，通过数据发掘提供详尽灵活的统计图、报表，从而辅助管理员进行安全信息审计。利用集中管理和数据分析系统，管理员可以高效地管理各 AG-6000 设备，全面掌握网络的整体安全状况。

2.9.1 设备集中管理

安博通集中管理和数据分析系统可以作为 AG-6000 大规模部署的集中管理平台，能够支持大规模的并发量。系统每隔 5 分钟就对这几千个网络节点进行轮巡，并且可以根据不同的轮巡时间对网络设备进行分组监测，这样就大大降低系统的并发监测数量，提升系统的性

能。

2.9.2 策略统一下发

安博通集中管理和数据分析系统具有策略统一下发能力，帮助管理员脱离苦海，集中新建七元组策略批量下发到每一台设备，对于政府、运营商、金融、电力和大型企业等分支结构众多的客户，可以极大的降低运维人员的工作量，帮助客户实现高效率管理运维。

2.9.3 采用高性能数据存储和查询

安博通集中管理和数据分析系统采用高性能数据仓库，此数据仓库是一款基于网格技术的列式数据库。简单易用，快速安装部署，使用中无需复杂操作，能大幅度减少管理工作；在应对 50TB 甚至更多数据量进行多并发复杂查询时，更能够显示出令人惊叹的速度。

安博通集中管理和数据分析系统支持 TB 级原始数据量的高性能查询，大数据量查询性能强劲、稳定：查询性能高，如百万、千万、亿级记录数条件下，同等的 SELECT 查询语句，速度比 MyISAM、InnoDB 等普通的 MySQL 存储引擎快 5～60 倍。高效查询主要依赖特殊设计的存储结构对查询的优化，帮助用户快速定位网络问题，查询各种条件的审计检索。高数据压缩比，能够帮助用户节省存储成本，支持普通 X86 服务器，无需专用硬件设备和存储，在某实验局没有采用集中管理和数据分析系统前日志存储 1 个月产生 500G 数据，而采用安博通集中管理和数据分析系统后，数据 1 个月存储减少至 60 多 G，这样大大节省了用户的存储硬件成本。

2.9.4 深层次数据挖据分析

安博通集中管理和数据分析系统采用了先进的数据挖掘分析技术，从收集到的大量数据当中进行深层的数据挖掘及分析，该子系统由日志代理、日志审计中心、日志数据库、审计系统管理器、日志分析中心五个部分组成。日志代理负责收集区域内各种操作系统、网络安全设备、应用程序的日志信息，过滤后发送给日志审计中心处理。日志审计中心负责接受区域内日志代理和各种安全设备、系统转发的日志信息，集中保存在日志数据库，日志分析中心负责对日志数据进行深度挖掘。

日志数据的深度分析工作主要由日志分析中心来完成。日志分析中心首先通过 ETL 处理，利用专用的数据抽取工具，将日志数据按照定义的规则，通过复杂的抽取、转换、清洗及聚合，最后装载至数据仓库 DW 中，生成满足多维分析的数据仓库数据，即事实表和维表。通过 OLAP 多维分析技术和 BI 前端展现工具，提供针对日志数据仓库的日常查询、统计报表、OLAP 分析、数据挖掘、KPI 统计分析和监控告警等决策分析功能，并将结果通过 WEB/GUI 方式展现给用户。

数据仓库是在企业管理和决策中面向主题的、集成的、与时间相关的、不可修改的数据集合。与其他数据库应用不同的是数据仓库更像一种过程，对分布在企业内部各处的业务数据的集合、加工和分析的过程。

数据仓库中包含 ETL、数据模型、信息展现等主要关键技术。ETL 是数据抽取（Extract）、清洗（Cleaning）、转换（Transform）、装载（Load）的过程。它是构建数据仓库的重要一环，用户从数据源抽取出所需的数据，经过数据清洗,最终按照预先定义好的数据仓库模型，将

数据加载到数据仓库中去。数据模型的重要性在于对数据做标准化定义，实现统一的编码、统一的分类和组织。标准化定义的内容包括：标准代码统一、业务术语统一。ETL 依照模型进行初始加载、增量加载、缓慢增长维、慢速变化维、事实表加载等数据集成，并根据业务需求制定相应的加载策略、刷新策略、汇总策略、维护策略。

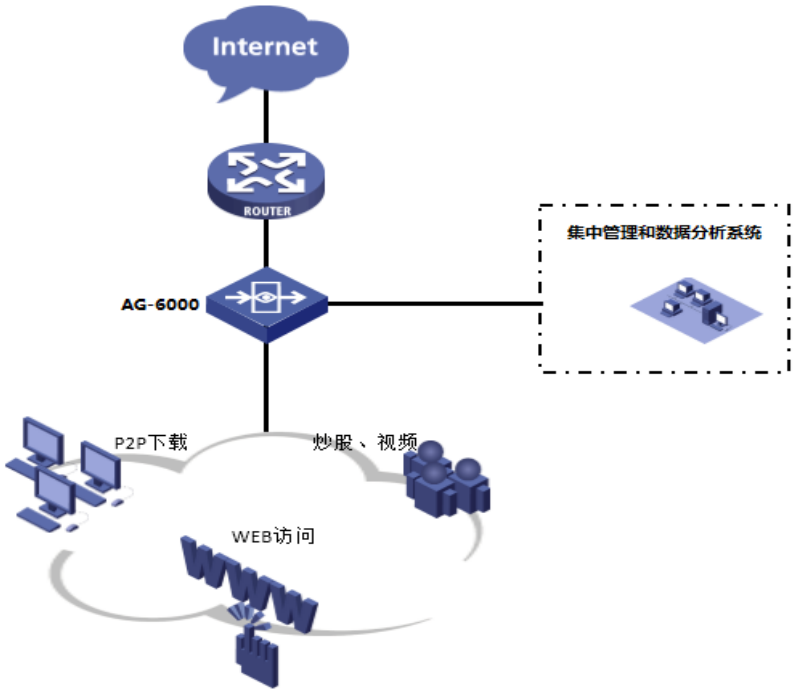
2.10 成熟稳定的数据库

审计功能每秒钟会产生数以千计的审计记录。为了使这些审计记录能被快速的统计，浏览，就需要使用数据库。目前我们使用的是比较成熟的 PostgreSQL 数据库。但是对于审计功能，记录量过于庞大，将这些记录放入同一个表格中显然不便于后续处理。所以，对于每个审计，我们每天创建一个表格。当天的数据会存放到对应的表格中，每天 0 点，会自动切换要入库的表格。

3 典型组网应用

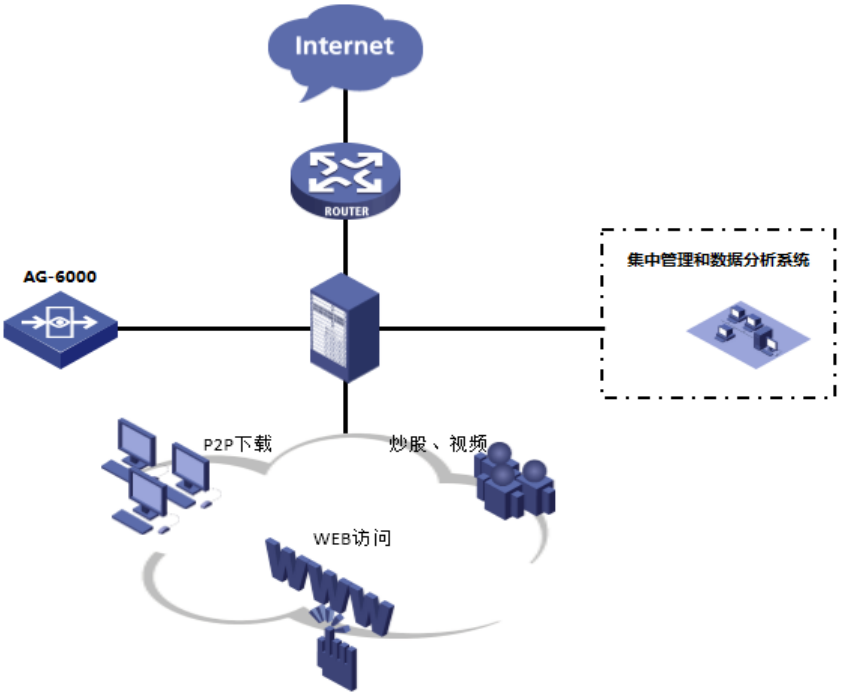
3.1 在线部署

- 适用于大中型企业用户，以透明方式在线部署于网络出口；无需改变网络拓扑；
- 对网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等各种应用进行监控和管理，保障关键应用和服务的带宽；
- 对用户上网行为进行分析与审计；
- 支持 VPN/MPLS/ VLAN/PPPoE 等复杂网络环境；支持设备本地日志记录和集中分析处理，可多台分布式部署统一管理；



3.2 旁挂部署

- 适用于大中型企业用户，以旁挂方式部署于核心设备旁；不影响网络结构，部署简单；
- 对用户网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等的流量、行为进行分析及审计；
- 支持设备本地日志记录和集中分析处理，可多台分布式部署统一管理；


Internet
ROUTER
AG-6000
集中管理和数据分析系统
P2P下载
炒股、视频
WEB访问

4 功能列表

分类	功能	详细指标
系统组成	系统组件	多核架构设计，系统硬件为全内置封闭式结构，稳定可靠，
组网部署	网关模式	支持路由模式接入网络
	网桥模式	支持透明、混合（透明+路由）、多组桥、多口桥
	旁路模式	单接口监听交换机镜像流量
接口配置	物理接口	启用/关闭
		IPv4 地址类型：静态（支持主从）、DHCP 动态获取 IP、PPPoE 动态获取 IP
		IPv6 地址类型：静态（支持主从）
		DHCP 下发 DNS
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		协商模式：自动、强制（可设置双工和速率）
		工作模式：路由模式、桥模式
		MTU，修改范围 1280-1500
	子接口	子接口管理（增删改查）
		子接口 ID：1-4094
		启用/关闭
		IPv4 地址类型：静态（支持主从）、DHCP 动态获取 IP、PPPoE 动态获取 IP
		IPv6 地址类型：静态（支持主从）
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		MTU，修改范围 1280-1500
	桥接口	桥接口管理（增删改查）
		桥接口 ID：0-255
		启用/关闭
		IPv4 地址类型：静态（支持主从）、DHCP 动态获取、PPPoE 动态获取
		IPv6 地址类型：静态（支持主从）
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		MTU，修改范围 1280-1500

	聚合接口	聚合接口管理（增删改查）
		聚合接口 ID：0-255
		启用/关闭
		IPv4 地址类型：静态（支持主从）、DHCP 动态获取、PPPoE 动态获取
		IPv6 地址类型：静态（支持主从）
		接口管理方式：HTTPS、HTTP、SSH、Telnet、Ping
		MTU，修改范围 1280-1500
	loopback 接口	支持生成、配置 loopback 接口。（命令行支持）
		支持基于 loopback（或指定 IP）接口地址的管理（设备管理等）（命令行支持）
	隧道接口（显示）	隧道模式：IPv6 隧道、Ipsec 隧道
		显示项目：接口名称、隧道模式、连接状态、启用状态
	4G 接口	支持联通 4G 上网卡（推荐：华为 E3372）
	TCP MSS 调整	支持根据业务类型智能调整
		命令行支持接口 TCP MSS 手工调整，支持全局设置和 VPN 单独配置
端口镜像	镜像接口	物理接口支持作为镜像接口和被镜像接口
	镜像功能	支持将多个物理接口的流量镜像到一个接口
		支持基于接口全部流量，上行流量，下行流量的镜像
DHCP	DHCP 服务类型	DHCP 服务器
		DHCP 中继代理
	服务器属性	网络配置：网关、子网、开始结束 IP 地址
		租约：无限、有限时长
		高级属性：DNS 支持 2 个，Wins 支持 2 个，域
		支持排除地址
		支持 IP-MAC 绑定
	DHCP 监视器	显示 IP 地址和 MAC 地址及开始时间、结束时间
		清除条目
IPv4 路由	路由表	显示设备路由信息
	高级路由属性	支持非对称路由
		命令行下支持强制源进源出
	静态路由	增删改查
		支持基于路由权重的多链路负载均衡
		支持路由优先级
		支持 VRF 配置
	策略路由	增删改查、移动
		5 元组策略路由+时间

		基于用户的策略路由
		基于应用的策略路由
		支持基于路由权重的多链路负载均衡
	ISP 路由	内置电信、联通、移动、教育网 SP 信息
		支持自定义 ISP 信息
		增删改
	RIP	支持 v1、v2
		支持缺省路由发布和路由重发布
		支持接口下发送版本和接收版本的设置
		支持认证方式：字符、MD5、不需要认证
	OSPF	支持缺省路由发布、路由重发布
		支持 OSPF 网络区域信息的增删改查
		支持接口下相关配置
		支持认证方式：字符、MD5、不需要认证
	源 NAT	支持配置的增删改查、移动
		源地址转换类型：出接口、地址池、 不转换
	目的 NAT	支持配置的增删改查、移动
		目的地址转换类型：地址池、转换端口、不转换
	静态 NAT	支持配置的增删改查、移动
	ALG	动态端口支持协议 ALG：H.323、SIP、FTP、TFTP、PPTP
		FTP、TFTP、SIP 支持非标准端口设置
	花生壳 DDNS	支持花生壳 DDNS 客户端以及域名 IP 绑定功能
	DNS-DNAT	支持负载在出接口的 DNS 请求主动完成 DNS 服务器替换
	基于流量权重 DNS 透明代理	支持 DNS 透明代理的 dns 请求根据接口流量负载完成接口选择
会话限制	规则管理	增删改查
	功能	支持基于地址对象的限制
		支持基于 IP 的会话数、每秒新建的限制（如引用地址对象，则对地址对象中的每个 IP 地址进行限制）
	限制阻断	显示限制信息
		IP 会话限制内容：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、引用地址对象名
		支持查询过滤和全部显示
	会话统计	显示当前 IP 地址的连接数
		支持 session 状态监控
地址探测	接口探测	支持 ping 地址监控条目
		支持 tcpsyn 地址监控条目
		支持 dns 地址监控条目
		支持接口类型：物理接口，子接口，桥接口，聚合接口，隧道接口
	地址探测组	支持多个地址探测从属组关系
		分为严格模式和非严格模式（严格模式即所有探测条目均成功组状态才成功，非严格模式探测条目间为独立状态）

		支持对探测组描述
	路由探测	支持探测路由以确保路由有效性
	支持场景及部署方式	支持静态路由或 ISP 路由联动
		支持与接口状态联动
		支持与 HA 联动
	日志说明	可对地址探测失效、恢复有日志记录
链路负载均衡	链路负载均衡	基于七元组的链路负载均衡策略
		基于域名的负载均衡策略
		基于接口，接口组的负载均衡策略
		基于直连网段和特定网段的负载均衡排除
		负载均衡接口支持 pppoe，dhcp，聚合链路，物理接口，等三层接口
		基于 ICMP 的接口探测机制
		支持基于源地址 hash 的链路负载均衡
		支持基于优先级的链路负载均衡
	VLAN	子接口都支持 IEEE 802.1Q，能进行封装和解封。
		支持对报文进行二次基于 802.1Q 封装的 VLAN-VPN 应用。（QinQ）
	生成树协议	支持 802.1d 的 STP 生成树协议。
	报文透传	支持二层解封装和再封装，对上层透明
	服务器负载均衡	支持一个公网 IP 映射到内网多台服务器，服务器间支持连接和源地址 hash，支持服务器健康检查
IPv6	基础功能	IPv6 路由通告
		IPv6 静态路由、OSPFv3
		支持用户和应用均为任意的 7 元组策略
		扩展报文头的逐跳报文的处理、分片报文等的处理
		隧道支持：手工隧道，6to4 隧道，ISATAP
		防畸形报文攻击
应用缓存	应用缓存	支持文件缓存
	APP 被动缓存	识别终端到特定服务器的 APP 下载，设备自动根据终端的下载地址下载 APP
	APP 模糊匹配	支持终端请求 APP 下载模糊匹配
服务质量管理	服务质量管理	支持 PING、TCP、DNS 探测
		支持接口探测
		支持自定义间隔时间探测
VRF	接口虚拟化	接口默认属于 root，创建 VRF 后可把接口添加到 VRF 内，一个接口只能属于一个 VRF；
	IP 地址重叠	不同 vrf 下的接口可以配置相同的 ip 地址
	静态路由	支持静态路由
通用功能	黑名单	支持手动配置
		支持触发防攻击规则和 IPS 阻断源地址规则自动进入黑名单
		支持生存时间配置
	攻击防护模块	扫描攻击分析

		异常包攻击分析
		Flood 攻击分析
扫描防护	通用	基于接口的配置
		支持自动加入黑名单
		扫描阈值设置
	扫描方式	端口扫描、IP 地址扫描
异常包防护	异常包类型	Ping of Death；Land-Base；Tear Drop；TCP flag；Winnuke；Smurf；IP 选项；IP Spoof；Jolt2
ARP 防护	防 ARP 攻击	启用与关闭
		支持 ARP 学习与主动保护
		可设置 IP-MAC 绑定
		防 ARP Flood 攻击
		支持 ARP 表查看、绑定、清除、接口信息
	ARP 学习控制	基于接口的 ARP 学习控制
Flood 防护	通用	一体化配置
		基于目的 IP、IP 范围
		支持接口防御
		阈值设置
	支持类型	SYNFlood、UDPFlood、ICMPFlood、DNSFlood
流量控制	线路管理	绑定接口
		支持基于接口的上下行带宽管理
	通道管理	支持高、中、低优先级通道设置
		支持应用、用户、源地址、服务、时间的通道匹配
		保障带宽
		限制带宽
		每 IP 限速
		自动支持流量整形
	流量时长日、月限额	支持日流量限额、时长限额，超过阈值提供弹窗提示且可自定义；支持流量和时长的月限额
	每用户流控	支持针对用户名实现每用户流控
排除策略	排除策略	支持用户、地址排除
IPv4 安全策略	配置管理	支持策略增删改查、启用/禁用、移动
		支持策略匹配次数清零
		支持修改默认策略动作：允许/拒绝
	策略	七元组策略匹配条件：用户、应用、源地址、源接口、目的地址、目的接口、服务
		支持基于时间表的策略配置
		支持应用选择过滤
		支持基于应用的应用类型组选择
		支持策略动作为：允许、拒绝、IPSec
		基于策略的长连接（老化时间）

		支持动作为拒绝的策略进行日志记录
IPv6安全策略	配置管理	支持策略增删改查、启用/禁用、移动
		支持策略匹配次数清零
		支持修改默认策略动作：允许/拒绝
	策略	支持任意的 7 元组策略
		支持基于时间表的策略配置
		支持策略动作为：允许、拒绝
		支持动作为拒绝的策略进行日志记录
应用过滤策略	配置管理	增删改查
		启用禁用
		描述
	策略	支持根据应用/应用类来区分不同的应用行为
		支持根据应用行为来区分不同应用的审计内容
		根据应用行为确定审计内容
		支持基于关键字或者数字的内容审计
		支持允许/阻断的策略动作
		审计日志选项:不记录、紧急、告警、严重、错误、警示、通知、信息
URL过滤策略	配置管理	增删改查
		启用禁用
		描述
	策略	支持恶意 URL 过滤
		支持预定义和自定义 URL 分类过滤
		支持 URL 阻断和审计（动作：允许 、拒绝）
		URL 日志选项:不记录、紧急、告警、严重、错误、警示、通知、信息
应用控制及审计	通用审计内容	审计用户名、所在组名
		审计应用名、所在应用类
		审计操作系统、平台、终端、供应商
		审计源 IP 地址、目的 IP 地址、目的端口
	即时通讯	基于帐号的登录控制、黑/白名单
		支持非加密收发消息时的关键字内容审计
	P2P 类	识别迅雷
	股票软件	基于行为（登录、交易、行情）的控制和审计
	网络游戏	基于行为的控制和审计
	搜索引擎	关键字过滤
	Webmail	支持邮件内容审计，不支持附件审计。
		支持普通版 webmail 审计（QQ、163、126、新浪、139 邮箱）
	社区类	支持论坛（BBS、博客）主题过滤（如果有）
		论坛（BBS、博客、微博）内容过滤
	联系人	支持以发件人过滤
	非加密邮件	支持邮件客户端的主题、内容、附件名过滤
		支持记录邮件内容，需要带本地硬盘

	命令类	支持基于命令和操作的审计
		论坛上传下载文件名过滤
https 解密	https 网页解密	支持预定义 https 页面解密
		支持自定义 https 页面解密
	ssl 加密邮箱解密	支持 ssl 加密网页版邮箱解密
		支持 ssl 加密客户端邮箱解密
	解密策略	支持解密策略的启用禁用
		支持基于入接口，源地址，目的地址多维度的解密策略
		支持解密策略排除特定的站点
PKI	证书格式	支持 X.509 V3 数字证书，支持 DER/PEM/PKCS12 多种证书编码。
	本地 CA	支持内置 CA，为其他设备或移动用户签发证书。
		支持本地 CA 根证书、根私钥的更新。
		支持在线 CRL 列表。
IPSec VPN	IKE 第一阶段协商模式	支持 IKEv1
		支持主模式和野蛮模式
	IKE 身份认证	预共享密钥
		RSA 证书认证
	加密/HASH 算法	国际标准算法(DES/3DES/AES;MD5/SHA-1)
	IPsec 冷备份	支持 Ipsec 冷备份，主 VPN 断开，备 VPN 触发开始建立
	IPSec 封装模式和协议	支持隧道模式
		支持 ESP 和 AH 封装
	部署模式	网关到网关
		远端地址为动态
		对端地址为 DNS
		Hub Spoke 组网，spoke 之间通过 IPSec 通信
		VPN track（可以探测到 VPN peer 地址不可达并将隧道删除）
		客户端远程接入，支持扩展认证和模式配置
		隧道 VPN
	配置方式	基于安全策略配置/基于路由（隧道口）配置
	其他特性	DPD
		NAT 穿越
		FQDN
		DH 组配置
		PFS
	维护手段	隧道监视器
	流量统计	支持隧道持续时间统计等
	用户功能	支持用户强制下线
	VPN 功能优化	提供 VPN 接口和 VPN 路由
		VPN 展示优化
		同设备对接和第三方对接
通用功能	导入导出	用户、组的导入导出
	新建、删除	用户、组的新建、删除

	用户组	支持用户组
	用户种类的改变	可以在认证用户、固定 IP 用户、匿名用户之间自由变换
	批量移动	支持一个或者多个用户的批量移动功能
	模糊查询	支持用户，用户组的模糊查找功能
	一键删除	支持一键删除所有的用户，用户组
	超时检查	对认证用户、移动用户、第三方认证用户支持超时时间检查
认证用户	账号管理	增删改查
	认证服务器	支持 HTTP 登录
	认证方式	本地认证、认证服务器、静态绑定
	认证设定	锁定时间
		认证用户保活
		支持唯一性检查
		登录后重定向页面
		绑定多个认证地址
	基本功能	用户登录和注销界面
		支持移动设备登录页面自适应
移动用户	用户	自动添加用户
	移动用户组	内置移动用户组
用户标签	用户标签	支持根据用户访问 URL 排名生成用户标签
第三方认证	支持伪 portal 抑制	支持通过 refresh 方式推送页面重定向
	https 弹 portal	系统认证支持 https 请求下弹出认证 portal，portal 认证支持 https 请求下弹出认证 portal
	支持 portal 联动	支持 portal 服务器联动，portal 服务器故障全部用户逃生
	radius 携带 nas-id	开发实现 NAS-Identifier(32)在无线场景携带 AC 名字
U-key 双因子用户认证	U-key 双因子用户认证	支持针对管理员登录设备开启双因子认证。
LDAP 用户管理	LDAP 用户同步	支持定时自动，手动的 LDAP 用户同步功能
		支持标准 AD 服务器和 OPEN LDAP 服务器的用户导入
	AD 域单点登录	支持同过策略实现标准的 AD 服务器单点登录
	LDAP 用户策略	导入的用户支持策略引用
识别相关	识别范围	设置识别的 IP 地址范围

重定向	重定向页面	默认重定向页面
策略	认证策略	匹配项：源接口、源地址、目的接口、目的地址、时间
		重定向页面选项（相关行为）
		支持微信、短信、本地、免认证、portal 认证
用户认证	微信认证	限制微信流量放通（pc 和移动端，认证通过放通）
		支持基于 http 获取 access_token
		支持微信内部浏览器 http 弹 portal
		强制关注功能（定时检查用户是否关注公众号）
	混合认证	支持本地、短信、微信、免认证四种认证方式的混合认证
	认证白名单	支持基于源地址的用户认证白名单
系统管理员	账号管理	管理员账号的增删改查
		只读管理员查看配置权限（审计员）
		登录认证方式支持本地认证、Radius 服务器认证、LDAP 服务器认证
		密码复杂度：必须包括数字，英文和字符，6-63 个字符
		每帐号可绑定 3 个 IPv4 地址或子网
	管理设定	支持三权分立
		支持账号唯一性检查
		最大登录重试次数 1-60 次，默认为 5 次
		登录失败阻断间隔 1-3600 秒，默认为 1 分钟
		页面超时时间 1-480 分，默认为 10 分钟
		在线管理员 1-20 个，默认为 20 个
	在线用户管理	支持管理员在线监控和强制下线
	阻断用户	支持管理员黑名单，阻断用户可监控，可解锁
	广告推送	支持 PC 端支持推送 4 个方位的广告，手机端支持推送全屏广告
认证服务器	Radius	支持用户信息在远端 Radius 服务器存储
		支持多用户第三方存储远端请求认证
		单服务器认证
	LDAP	支持用户信息在远端 LDAP 服务器存储
		支持多用户第三方存储远端请求认证
		不支持 LDAP 组同步认证
		支持 LDAP 用户、用户组同步
		单服务器认证
	服务器组	Radius/LDAP 服务器组，支持主备和集群
	短信认证	支持短信验证码验证身份实现 wifi 认证上网
		短信网关认证页面自定义
	微信认证	支持微信关注公众账号实现 wifi 认证上网
		支持二维码扫描认证
	免认证	免认证
	无感知认证	无感知认证（非跨门店）
	系统时间	手工设置时间
		NTP 同步

系统维护设定		设备间同步时间（通过 NTP 保持一致）
	系统重启	恢复出厂配置
		系统重启
	部署方式	旁路部署
	授权	许可证
	配置文件	配置文件导入导出
		双备份配置
	系统升级	系统升级手动、自动、升级历史
		支持断点续传
		动态库升级（应用、URL、IPS、AV）
	诊断工具	ping 探测
		traceroute 探测
		TCP SYN 探测
	抓包工具	支持按照过滤条件抓取数据报文
		支持将报文下载到本地保存查看
	U 盘零配置启动	支持设备重启阶段读取文件格式为 FAT32 格式的 U 盘配置，作为系统启动的配置
	多配置管理	支持命令行下多配置管理
	信息收集	设置方式：手动搜集和自动收集
		收集内容操作：下载、查看、删除
可靠性	硬件 bypass	电口断电 bypass
		电口启动过程 bypass
	软件 bypass	IPS 模块软件 bypass：瞬时 cpu 使用率超过 70%按 10:1 进入检测流程
双机热备 HA	主备模式	支持配置同步
		支持流同步
		支持特征库同步
		支持接口状态监控
		支持抢占模式
		支持备机可管理
		支持业务口作为心跳口，提高心跳口可靠性
		支持 HA 状态监控
	主主模式	支持认证用户同步
		支持流同步
		支持接口状态监控
		支持地址代理
		支持非对称路由
		支持业务口口作为心跳口，提高心跳口可靠性
接口状态同步组	物理状态同步	支持两个或者多个接口状态绑定
SNMP	SNMP 配置	SNMP 代理

		版本：v1、v2、v3
	trap	trap 版本：v1、v2 Notification、v2Inform
		trap 地址
	私有 mib	CPU、内存
	SNMP 用户	增删改查
		认证方式：None、MD5、SHA
	支持跨三层 IP MAC 绑定	支持跨三层 IP MAC 绑定
域名相关	DNSserver	支持 4 个 DNS 服务器
		静态域名（256 个）
	DNS 透明代理	代理接口支持三层接口
		实现基于优先级的 dns 代理算法
		实现基于权重的 dns 代理算法
		支持静态域名配置
		支持特定域名特定 dns 服务器解析
		静态域名和特定域名支持模糊匹配
		支持 dns 透明代理缓存管理
日志设定	syslog 日志配置	日志服务器：地址和端口（3 组）
	日志过滤	本地认日志记录开关、日志服务器日志级别开关
	设备映射表	设备映射表流量、上网行为、系统管理
Debug	命令行	各模块 Debug 支持
管理端口漂移	cli 端口：telnet ssh	支持命令行管理端口的漂移
	WEB 端口：80；443	支持界面管理端口的漂移
无线非经	数据库表	支持本地生成用户终端上下线、上网日志、普通内容、AP 资料、场所资料、虚拟身份、搜索关键字信息、BBS 信息、Email 信息等数据库表；
	对接平台厂商	支持国标（GA/WA3011.1-2015）数据格式对接；
		至少支持任子行、派博、爱思、虹旭、锐安、网博、中新、恒邦、兆物、云辰、宽广智通、携网等主流后端公安平台的直接对接（非额外部署日志服务器方式对接，需提供 web 截图证明）；
	认证数据	支持标准的 radius 服务器；
		支持非标准的 UDP 9999 端口获取用户认证信息；
		支持主动读取部分 AC MIB 库方式获取用户信息；
		至少支持与城市热点、深澜、泰联、光华冠群、华三 IMC、SAM、安美等认证服务器；
	跨三层审计	#支持烽火、普天、长虹、海信等胖 AP 的用户溯源审计；
	数据上报周期	支持数据实时上报，同时可根据用户要求设置上报时间周期；
	标准 API 接口	#支持与标准的电信 CRM 系统进行对接，可主动获取场所和 AP 等信息；
	数据传输	支持 FTP、FTPS、HTTP、UDP 等方式传输

		支持.ZIP、.syslog、.XML、.bcp、.ok 等文件格式
		支持标准的 CBC 模式的 DES 加密算法
首页	系统信息	设备序列号、主机名称、产品型号、系统版本、URL 版本、APP 版本、IPS 版本、AV 版本
		系统时间、日志汇总（访问网站、收发邮件、论坛与微博、IM 聊天）、当前会话数、运行时间
	实时流量（设备）	基于物理口的上下行流量统计 bps（1 小时 60 个点）
		整机总流量统计 Kbps/Mbps/Gbps
	接口信息状态	接口状态
		接口详细信息
	用户、应用流量排名	Top 15
	系统资源	CPU、内存
在线用户	全部用户	显示所有用户
	移动用户	显示移动用户
	查询	按网段查询
	管理	冻结、解冻
		离线
防私接防共享	防私接防共享	支持基于 IP 及 IP 段配置白名单
		支持 基于用户、MAC、终端数量的监控
		支持状态监控、解锁操作
统计集	应用流量统计	应用统计总览可视
		应用比例图呈现
		应用统计趋势图总览
		应用统计详细信息展现
		应用与用户维度耦合
		应用 TOP10 统计
	用户流量统计	用户统计总览
		支持用户统计柱状呈现
		用户统计详细信息总览与应用维度耦合
		支持查看单个用户的应用趋势及应用 TOP 列表
		用户 TOP15 统计
流量监控	接口流量统计	支持接口上下行统计，包含每小时、每天、每周
		支持设备转发数据历史的可视化
		支持每个接口收发数据历史的可视化
	用户信息中心	支持时间轴方式记录账号网络访问过程
		支持将客户多种审计条件统一管理查看
	健康统计	支持对设备转发流量统计，cpu 使用率，内存、会话、转发流量 4 项统计趋势图
		支持时间选项查阅历史使用情况
地址	IPv4 地址对象	增删改查，支持批量删除
		支持子网、地址范围、主机的地址添加方式
		支持排除地址

	IPv6 地址对象	增删改查，支持批量删除
		支持子网、地址范围、主机的地址添加方式
	地址组对象	增删改查，支持批量删除
		支持组嵌套
服务	预定义服务	支持 89 种预定义服务
	自定义服务	增删改查，支持批量删除
		支持协议类型：TCP、UDP、ICMP、其他协议号
	服务组	增删改查，支持批量删除
		支持预定义自定义服务添加
		支持组嵌套
	非标准端口配置	非标准端口 ALG（FTP、TFTP、SIP）
应用	预定义应用	显示预定义分类，支持 18 个分类
		基于 IP，端口，协议完成自定义应用
		显示分类下应用的属性：中英文名称、平台、风险级别、流行度、描述
	应用组	增删改查
	识别模式	支持修改识别模式以达到对应识别目的
		智能模式：应用引擎将尽可能多的方法识别应用流量
		快速模式：应用引擎关闭部分智能分析以提高性能
		关闭模式：应用引擎关闭
时间表	通用	增删改查，支持批量删除
		内置任何时间条目：any
	时间类型	日计划、周计划、月计划
		计时器
URL	恶意 URL 白名单	支持对恶意 URL 手工排除
		支持 URL 过滤黑白名单简单配置
	预定义	查看预定义 URL 分类
	自定义	增删改查，支持批量删除
关键字	自定义	增删改查，支持批量删除
数据库	嵌入式数据库	分类记录
		日志存储空间耗尽后，可滚动覆盖
日志记录	事件日志	系统关键事件日志，支持中文显示
	管理日志	管理员操作日志，支持中文显示
	安全日志	攻击防护日志，支持中文显示
	IPS 日志	IPS 日志，支持中文显示
	AV 日志	AV 日志，支持中文显示
	业务告警	支持针对设备监控状态，VPN 信息等维度告警，告警事件入库支持展示，查询，导出；告警事件支持弹窗，邮件；弹窗默认展示最近 10 条告警记录
网站日志	访问网站日志	支持记录 html 编码格式为 UTF-8 和 GBK2312 的网页 title；支持日志导出；支持中文显示

		支持超链接直达客户所访问网页；支持日志导出；支持中文显示
		不记录无意义 URL 日志（如内嵌广告）；支持日志导出；支持中文显示
		查询，可自定义查询条件；支持日志导出；支持中文显示
	恶意 URL 日志	查询，可自定义查询条件；支持日志导出；支持中文显示
应用审计日志	IM 聊天软件日志	查询，可自定义查询条件；支持日志导出；支持中文显示
	社区日志	查询，可自定义查询条件；支持日志导出；支持中文显示
	搜索引擎日志	查询，可自定义查询条件；支持日志导出；支持中文显示
	邮件日志	查询，可自定义查询条件；支持日志导出；支持中文显示
	命令日志	查询，可自定义查询条件；支持日志导出；支持中文显示
	其他日志	查询，可自定义查询条件；支持日志导出；支持中文显示