上网行为安全审计产品

技术白皮书

上海弘积信息科技有限公司

目录

1 产品概述

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。这些单位面临着高法律和经营风险 ,可能为此蒙受巨大损失 ,如何才能有据可查 ,合法合规。网络流量增大、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。企业快速的更新换代导致运维力量顾此失彼，快速高效的解决运维问题是企业成长面临的重要问题之一。难以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。

弘积上网行为安全审计是业界识别最全面、控制手段最丰富的高性能应用控制网关。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，并利用智能流控、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、清晰易用的管理日志功能等，提供业界最全面、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，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。

1.1 灵活高效全面，场景支持更丰富

弘积上网行为安全审计搭载自主可控的防火墙系统，融合了丰富的网络特性，在满足 IPv4/IPv6 双协议栈的同时，配合智能路由和 DDNS 等，可在 802.1Q、RIP、OSPF 等各

种复杂的网络环境中灵活组网；具备与第三方系统对接，数据共享，提升业务价值。弘积上网行为管理具备优秀的适应性，适用各种复杂场景，更符合业务需要。

领先的多核架构及分布式搜索检测引擎，配合高性能的处理器，多业务并行处理，确保弘积上网行为管理在各种大流量、复杂应用的环境下，仍能具备快速高效的业务处理和防护能力。

弘积上网行为安全审计集防火墙、负载均衡、入侵防御、病毒过滤、应用识别、行为控制、VPN 接入、业务可视、安全认证等功能于一体，为用户提供了一个灵活、高效、全面的网络解决方案。

1.2 用户认证多样，用户管理更便捷

弘积上网行为安全审计提供了丰富的用户认证方式以及用户同步方式，支持本地认证、短信认证、微信认证、AD 单点登录、APP 认证、二维码认证等多种准入认证，以及 AD 服务器、Radius 服务器、Portal 服务器等外接外部认证服务，更好的满足企业对于用户管理要求。

弘积上网行为安全审计具备高效的 Portal 推送功能 ,支持 https 网站推送 Portal 页面；通过伪 Portal 请求抑制可减轻 Portal 服务器压力，解决客户 Portal 推送痛点。

弘积上网行为安全审计提供丰富多样的用户录入功能，静态和动态的用户录入方式，满足各种用户录入场景和用户管理诉求。

1.3 应用控制细粒度，行为管控更精细

弘积上网行为安全审计采用 DPI/DFI 融合识别技术 ,通过对用户流量进行全面的分析，能够深入识别应用的内置动作，系统内置 4500+应用，可以基于应用完成细粒度的应用控制。

可以对 IM 聊天、搜索引擎、论坛社区、邮件收发、文件传输、娱乐股票等模块的应用行为、内容、状态等进行细粒度审计，支持 QQ 和微信聊天内容审计、传输文件还原、文件大小设置。通过应用精细化管理让网络更有序。

弘积上网行为安全审计可对关键信息进行审计，包括网页访问行为、网络发帖、邮件 Email、IM 聊天内容、文件传输、游戏行为、炒股行为、在线影音、P2P 下载等行为，并且包含该行为的详细信息等。为防止企业关键信息泄露，提高网络安全性提供保障和依据。

1.4 带宽优化管理，用户体验更迅速

企业单位的出口带宽有限，带宽使用情况的不清晰不准确，造成了带宽未能有效的利用起来，带宽资源白白的被浪费掉。弘积上网行为安全审计能帮助组织管理者透彻了解组织当前、历史带宽资源使用情况，并据此制定带宽管理策略，验证策略有效性。不但可以在工作时间保障核心用户、核心业务所需带宽，限制无关业务对资源的占用，亦可以在带宽空闲时实现动态分配，以实现资源的充分利用，提升用户使用网络的体验。流量限额和时长限额区分用户权限，实现差分服务，助力营销。

1.5 增值营销特性，营销推广更精准

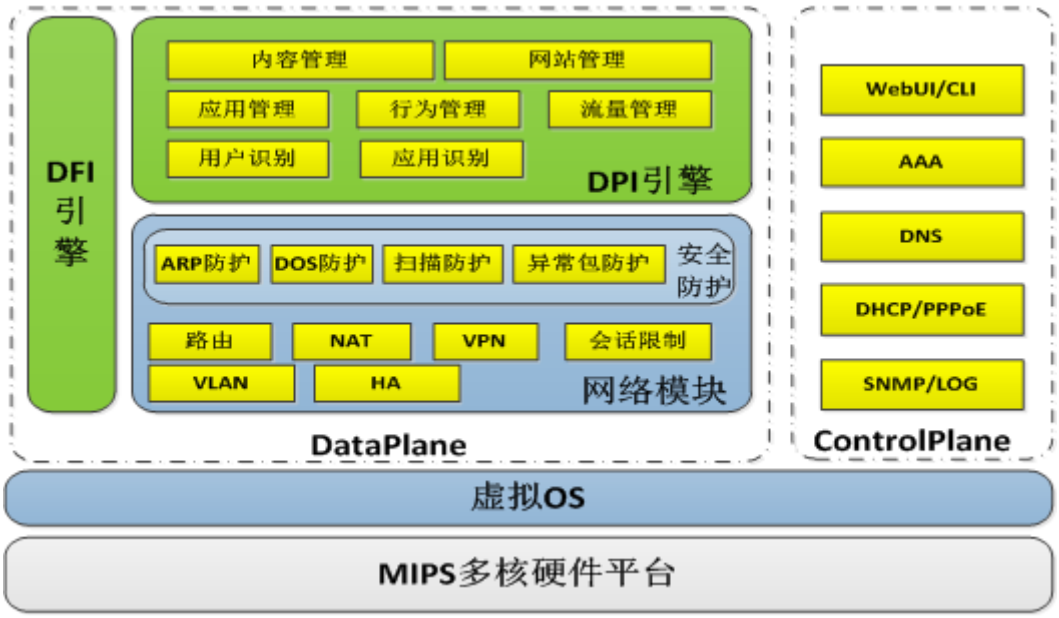
弘积上网行为安全审计以“人”为单位进行风险控制和业从用户出发智能关联分析，形成“日志跟踪轨迹”；通过智能的用户报表系统，内置多套报表模板，适应各种场景，同时支持报表订阅和实时报表功能，实现多维度、全方位的实时统计分析。通过大数据分析实现精准营销推广，实现网络资源的合理利用的同时，提升数据价值。

弘积上网行为安全审计提供针对终端定时循环公告推送，公告页面支持管理员自定义，可基于策略进行公告推送，保证受众用户精准。

2 技术实现

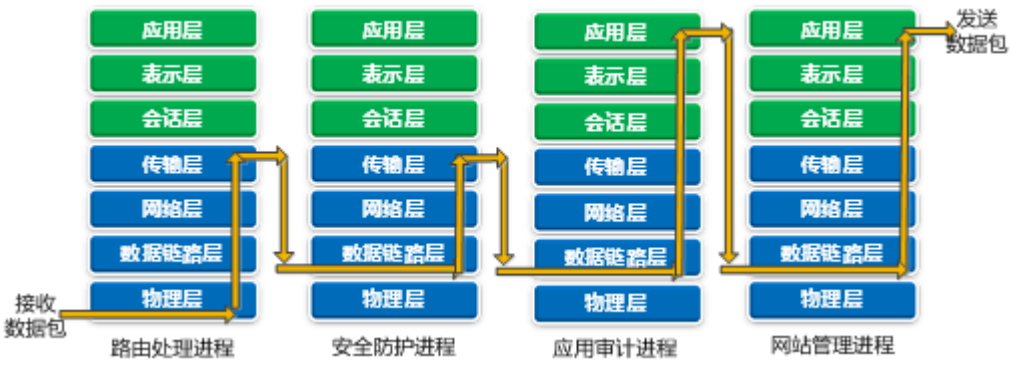
2.1 MIPS多核架构

弘积上网行为安全审计采用了 MIPS（单字长定点指令平均执行速度 Million Instructions Per Second 的缩写，每秒处理的百万级的机器语言指令数。这是衡量 CPU 速度的一个指标。）多核架构。在硬件架构上运行了虚拟 OS（操作系统），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。

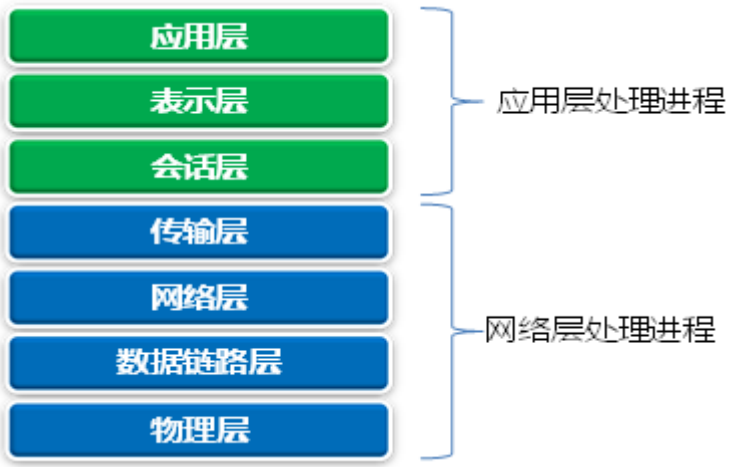


- 数据面

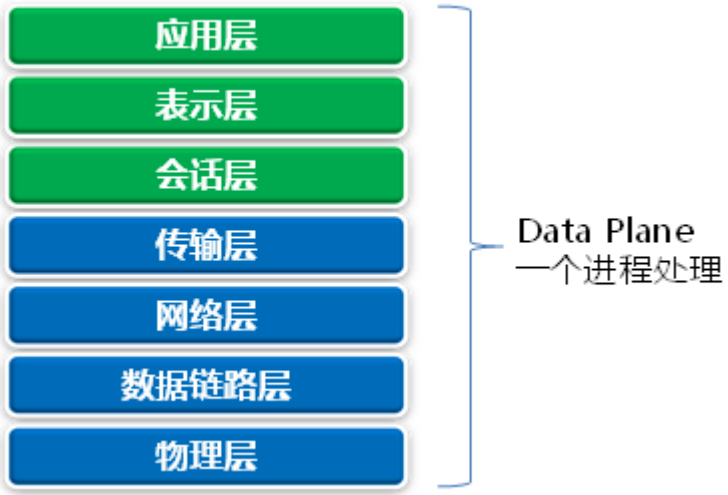
传统的网关设备为了降低设计和开发难度，会将各个模块以进程的方式存在，数据包每通过一个模块都要重复对数据的解析。增加了数据包在系统停留的时间，从而造成了网络延迟大的问题。



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。



弘积上网行为安全审计的 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启解析数据包所消耗的资源，从而降低网络延迟。



2.2 网络特性

2.2.1 部署模式

弘积上网行为安全审计支持透明、路由、旁路和混合等部署模式，可灵活的连接和审计用户网络。

- 弘积上网行为安全审计透明模式接入用户网络，部署于关键节点，网络拓扑改动较小，对经过的数据流量进行分析，实现对用户行为的审计和控制；
- 弘积上网行为安全审计路由模式一般使用在公网出口或三层交换节点，提供 NAT、负载均衡等出口特性，并对内网用户实现 VPN、流量管控、行为审计和控制等功能；
- 弘积上网行为安全审计旁路部署不会影响客户现有网络结构 ,通过与交换机镜像接口连接，将需要审计的网络流量镜像至弘积上网行为安全审计中，实现分析和审计用户行为的功能；
- 弘积上网行为安全审计支持混合模式，即同时使用透明、路由、旁路模式，用于满足用户复杂多样的环境需求。

2.2.2 支持的路由特性

网络的迅猛发展 ,网络设备的静态路由已经无法满足企业网络实时自适应网络结构变化的需求。弘积上网行为安全审计用户提供丰富的路由协议，支持静态路由、策略路由、ISP 路由，RIP、OSPF、VRF 等路由功能，以满足用户复杂的网络环境。

用户出口有多个运营商线路时，跨运营商线路访问资源时，会出现网络访问缓慢，服务质量下降等问题。弘积上网行为安全审计 ISP 路由主要用于解决此问题。弘积上网行为安全

审计预置中国电信（ChinaTelecom）、中国联通（Chinaunicom）、教育网（ChinaEducation）、中国移动（ChinaMobile）四个主流运营商的地址库，支持自定义增加 ISP 条目。管理员可指定运营商和出接口，当访问请求解析后按照预定的出接口或下一条进行转发，从而使得业务质量最优。

2.2.3 负载均衡

2.2.3.1 链路负载均衡

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弘积上网行为安全审计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，弘积上网行为安全审计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

弘积上网行为安全审计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。

- 智能应用路由

弘积上网行为安全审计内置超过 1500 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。

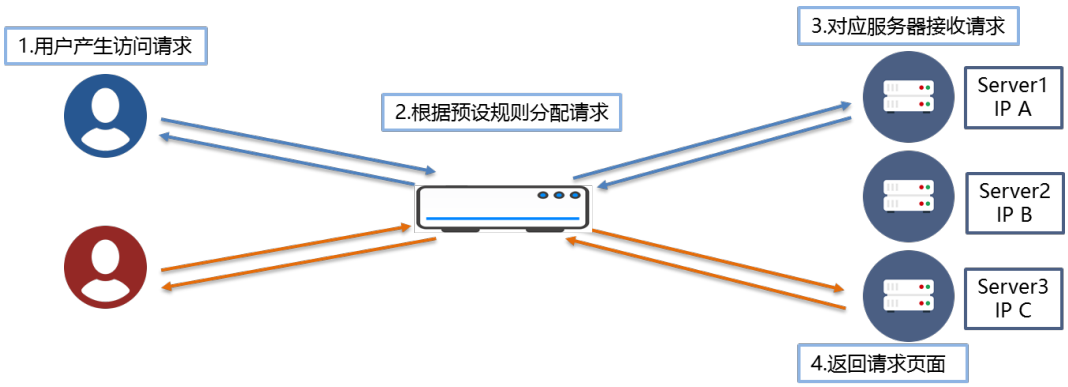
2.2.3.2 **服务器负载均衡**

弘积上网行为安全审计服务器负载均衡可以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。

弘积上网行为安全审计能够实现在客户访问多台同时工作的服务器的情况下 ,即时按需动态检查各个服务器的状态 ,根据预设的规则将请求分配给最有效率的服务器 ,实现数据流合理的分配 ,使每台服务器的处理能力都能得到充分的发挥 ,提高整体性能 ,改善应用系统的可用性。

弘积上网行为安全审计服务器负载均衡包含三个基本元素：

- 负载算法：权重算法、源地址散列+权重算法
- 服务器健康检查：提供 ICMP 和 TCP 两种探测方式
- 会话保持功能：可保持用户所有访问会话分配至同一台服务器上处理



2.2.4 地址转换

弘积上网行为安全审计拥有优化过的 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。

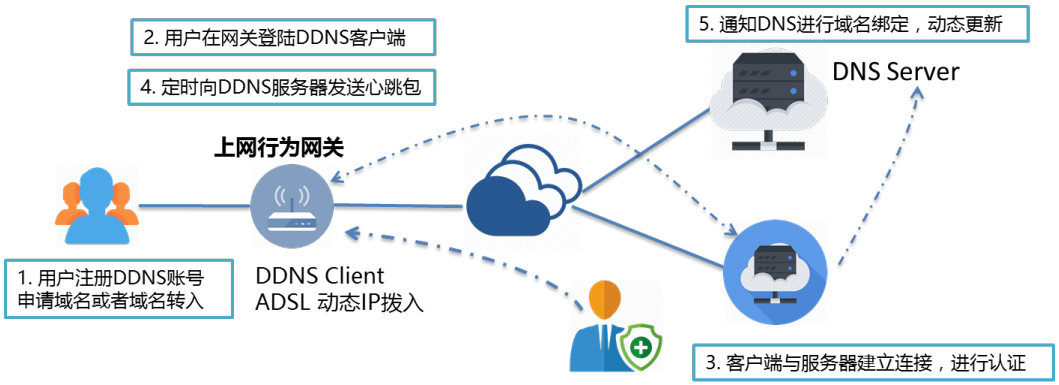
弘积上网行为安全审计针对内网通过公网域名或 IP 地址访问内网服务器的场景，支持 NAT 回流，管理员只需要在对应的目的 NAT 策略勾选 NAT 回流选项即可。系统会默认处理以上场景。

2.2.5 动态域名服务

DDNS（Dynamic Domain Name Server）是动态域名服务的缩写。动态域名服务是将用户的动态 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，动态域名服务提供了解决方案，它可以自动更新用户每次变化的浮动 IP，然后将其与网络域名相对应，这样其他上网用户就可以透过网络域名来交流了

弘积上网行为安全审计提供动态域名服务功能。可解决动态 IP 地址场景下管理，以及 IPsec VPN 场景使用域名连接等问题。



2.2.6 虚拟化功能

2.2.6.1 网络功能虚拟化

弘积上网行为安全审计支持网络功能虚拟化（NFV），并且支持 KVM、VMware ESX 等业界主流虚拟化环境。

NFV 技术使得弘积上网行为安全审计打破功能模块依赖于硬件的局面，安全资源可被充分利用，新业务开通上线快、部署灵活。可基于客户实际业务需要进行弹性伸缩。可应用于运营商、云服务商、数据中心、园区网等多种场景。更低成本的解决方案，开放的 API 接口，可为客户获得更多、更灵活的网络能力。

2.2.6.2 VRF 路由

在传统网络中 如果网络中有较多的网络部署划分 就可能需要部署多台出口路由设备，不仅建设成本高，而且占用更多宝贵的机房空间，维护成本和难度也居高不下。

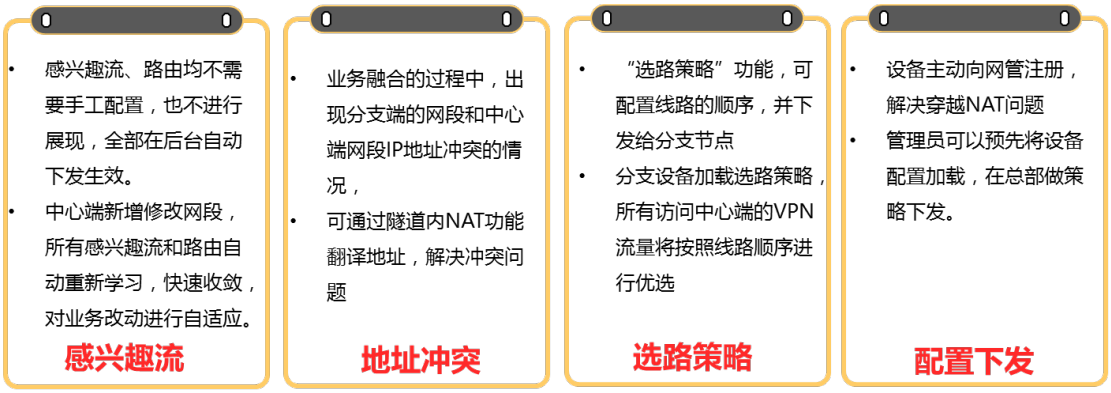
传统路由设备的不足，推动了虚拟化技术的普遍发展。弘积上网行为安全审计迎合网络时代潮流 ,自主开发了 VRF 功能。弘积上网行为安全审计可以将不同的端口加入创建的 VRF 组中，每个 VRF 组之间可以独立控制和转发，相互隔离，可以看做是不同的路由器，可以

使用相同的或者是重叠的 IP 地址而不会产生冲突。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，可以为用户节省大量的建设成本和维护成本，维护也更加简单。

2.2.7 快易 IPsecVPN

弘积上网行为安全审计的 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。

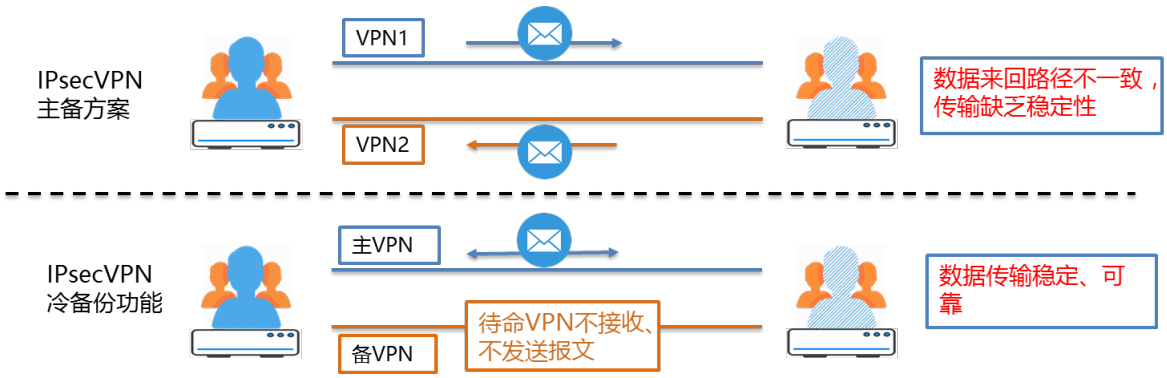
对金融、能源、交通等行业一些分散型的营业网点，对于业务连续性以及内网数据安全要求非常高。在租用运营商的固网光纤专线作为主链路的同时，还需一条安全稳定的备份链路以应对突发状况，专线成本高、灵活性差的缺点暴露无遗；弘积上网行为安全审计支持 4G 网络并支持 4G IPsec VPN 加密连接进行链路备份。连接提供按需拨号，无需改变原有网络架构，在主线路故障时主动承接和中心端的网络加密通信，具备数据完整性、数据传输安全、高性价比、网络无改变等特性。



2.2.8 IPsecVPN 冷备份

IPsecVPN 一般会承载客户关键数据，业界为了保障其可靠性，会使用 IPsecVPN 主备方案。但该方案在特殊场景中由于主备链路的 SA 阶段均处于 UP 状态，所以会导致数据包来回路径不一致，隧道稳定性较差的问题。

弘积上网行为安全审计创新性的推出了 IPsecVPN 冷备份功能，该功能设定待命 VPN 隧道不接受和发送报文，避免了数据包来回路径的问题。弘积上网行为安全审计提供数据加密的同时，提升了数据传输的可靠性，避免业务损失。



2.3 管理特性

2.3.1 设备管理

2.3.1.1 双因子设备管理

传统的账号密码设备管理方式安全性较低，容易被黑客截获破译，且认证唯一性难以保障。弘积上网行为安全审计提供双因子认证功能，用户登陆设备界面时，需在 PC 终端插入 U-Key，同时进行账号密码校验；否则无法登陆设备界面。

此功能极大的提高了网络设备的安全性，且具备操作简单，携带方便的特点。

2.3.1.2 中英文切换

弘积上网行为安全审计内置中文、英文两种语言，管理员可根据场景需求，切换使用界面的语种。

2.3.1.3 三权管理

弘积上网行为安全审计默认管理模式为普通模式，普通模式默认存在 admin 账号，该账号可添加、修改、删除所有管理账号，且可管理所有界面模块，无细致权限划分。

弘积上网行为安全审计可将管理模式切换为三权模式。切换后系统默认存在四种管理账号：

- 权限管理员（Authority），为系统管理员分配权限，可设置读写分离，支持设置模块分离管理
- 账号管理员（Account），添加、删除管理员账号
- 审核员（audit），查看所有管理员操作记录
- 管理员（admin），系统功能配置与管理

每个管理账号被赋予不同的权限，相互之间形成权限制约，避免了普通模式下超级管理员权限过大带来的管理风险，保障了设备管理安全。

2.3.1.4 管理方式

弘积上网行为安全审计本地管理支持多种管理方式，且所有接口均可用于系统管理，管理方式包括 PING、HTTPS、TELNET、SSH、HTTP 等。

2.3.2 用户管理

用户是上网行为安全最核心的要素，任何一条策略都是针对一个用户或者部门设置的，因此对于用户的识别、认证与管理能力决定了上网行为安全审计的效果。 弘积上网行为安全审计提供了丰富的用户认证方式以及用户同步方式 ,标准的树形结构用户管理方式更好的满足企业对于用户管理要求。

弘积上网行为安全审计的用户类型有：第三方用户，匿名用户和认证用户，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。用户支持丰富的导入方式包含 :标准的 AD 用户同步、SNMP 用户扫描导入、ARP 用户探测导入、认证后自动录入以及传统的 Excel 自定义导入功能用户管理更便捷、更全面。

2.3.2.1 树形组织结构

当用户数目较多、组织结构比较复杂时，按照实际的阻止都管理用户是最有效的方式，抑郁管理员查询、定位和设置策略。弘积上网行为安全审计支持标准的树型结构管理用户，能够完全按照企业的实际情况建立用户组织关系。如下图：

2.3.2.2 用户属性组

弘积上网行为安全审计系列支持属性组用户。属性组用户是指将某些具有一定公共特征（如部门、职位、电话、性别、年龄等）的用户以属性组的方式进行保存，网络管理员可以从属性维度对用户进行管理，例如：同通过策略方便实现某一部门男性经理禁止访问淘宝等功能。

2.3.2.3 临时账号

弘积上网行为安全审计系列支持本地临时账号。临时账号是指针对本地创建的用户账号设置一个有效时间，当超过有效时间段则账号自动失效。网络管理员可以针对部分临时员工设置临时账号。如此设计可以最大限度的降低账号外泄的风险。

2.3.2.4 用户认证后自动录入

弘积上网行为安全审计系列支持用户认证之后自动录入本地组织结构，方便认证用户的精细管控。针对目前支持的所有认证方式全部支持用户认证之后自动录入本地，这样认证之后的用户就可以作为本地用户展开精细化管理控制。该功能主要场景是针对用户信息在行为管理设备外部的。

2.3.3 身份认证

弘积上网行为安全审计具备丰富身份认证方式，可有效的区分用户。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。

弘积上网行为安全审计的身份认证方式有：

- 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；
- 免认证：认证用户无需进行身份认证，即可快速上网；
- 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：强制关注，自动弹出“一键微信连 WIFI”并关注微信公众号；
- 混合认证：界面配置选择多种认证方式，用户可根据需要更换认证方式；
- 单点登录： AD 域一次认证，减免频繁认证。
- 二维码认证：访客网络安全，管理授权网络访问。

2.3.3.1 **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 ACG 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，弘积上网行为安全审计支持二次到店免认证，直接关联上 SSID 即可自动认证通过并上网，用户无感知；管理员可选择配置强制关注，认证时必须关注公众号，否则无法正常使用网络；给用户超预期的体验，提高企业品牌认可度。

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。

2.3.3.2 APP 认证

近年来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弘积上网行为安全审计预定义配置 APP 特征，弘积上网行为安全审计会根据此 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，弘积上网行为安全审计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。

2.3.3.3 AD 域单点登录

大型企业中，内网用户均需进行 AD 域身份校验，若内网同时存在其他身份验证，用户需逐次进行认证，且操作步骤繁琐。弘积上网行为安全审计可与企业 AD 域进行联动，内网用户只需一次认证，即可完成所有身份校验，简化认证步骤，提升用户体验。

2.3.3.4 访客二维码认证

针对目前市场端出现的非经无线网络和大型企业访客网络 ,在网络访问方便的同时也存在一定的网络安全隐患。传统的认证方案已经不适用这样便捷的网络。快捷方便的二维码认

证因用而生，只需要已经认证的用户终端扫描未认证终端的二维码信息。即可协助未认证终端完成认证。

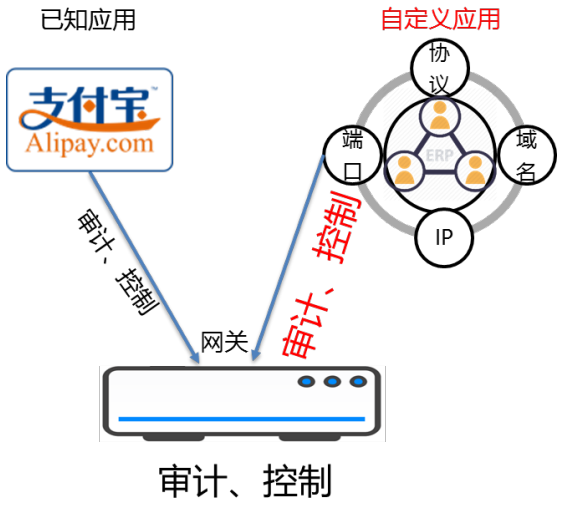
2.3.4 应用识别

应用识别（Application identify)是弘积上网行为安全审计的重要功能。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：

2.3.4.1 自定义应用

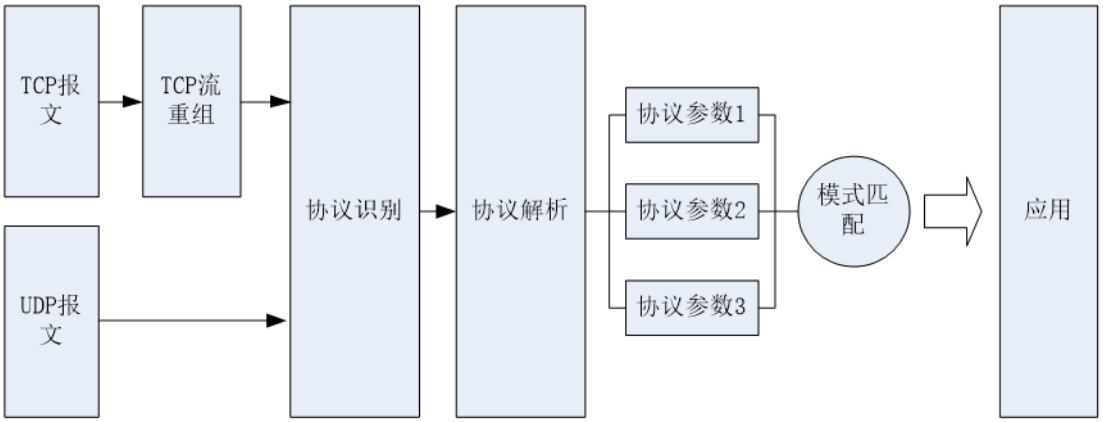
办公自动化的趋势下，客户内网均已搭建了企业的应用系统，例如 OA、ERP 系统等。面对这种情况，弘积上网行为安全审计通过自带的应用特性库无法对企业应用系统机型识别、审计和管理。弘积上网行为安全审计具备自定义应用功能，管理员可根据协议、目标端口、IP、域名等维度创建应用特征，进而针对企业应用进行审计、流量统计和控制。



2.3.4.2 基于协议状态分析

弘积上网行为安全审计对已知协议和 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。



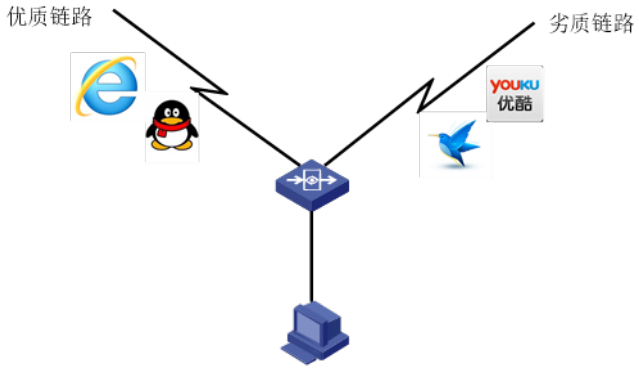
2.3.4.3 行为检测

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。

2.3.4.4 应用路由

弘积上网行为安全审计通过配置策略路由，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。



弘积上网行为安全审计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。

2.3.4.5 基于应用的流量管理

弘积上网行为安全审计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。

2.3.4.6 精准的应用控制策略

随着网络应用的日新月异，应用精准控制的需求愈发强烈，弘积上网行为安全审计提供精准的应用控制功能，应用控制粒度集中体现了应用的识别能力。

弘积上网行为安全审计提供多种应用的精细化控制：

- 应用控制

系统内置的应用对象精细化到应用具体的动作，管理员可以根据网络需要针对应用实现网路允许和网络阻断。相关行为可以触发对应的日志记录。

- 邮件控制

针对邮件发送支持针对发件人和收件人支持黑白名单控制，针对邮件标题和邮件内容支持关键字过滤；针对邮件整体大小支持管理员自定义大小，范围支持 0-100M；针对附件个数同样可以控制，范围支持 0-100 个。相关邮件行为可以触发对应的日志记录。

- Web 关键字过滤

关于 Web 关键字控制主要覆盖三种常见场景：搜索引擎；HTTP 上传；网页内容。以上场景全部支持。功能实现所见即所得。配置更加清晰。

- 虚拟账号

针对虚拟账号支持黑白名单过滤。目前弘积上网行为安全审计主要支持针对 QQ 账号的控制。后期会根据市场需求逐渐叠加微信、微博等相关模块的账号控制。

2.3.5 应用审计

弘积上网行为安全审计系列行为管理设备基于应用识别的基础可以实现应用中相关内容的审计，记录。常见的审计内容包括电子邮件类、即时通讯类、网络论坛类、博客类、网购类、微博类等应用。弘积上网行为安全审计行为管理设备通过用户上网的流量解析，将上述应用的交付内容和关键信息全部采集下来，例如 QQ 号、上下线时间、论坛发帖内容、网购搜索内容等。协议类识别

当弘积上网行为安全审计设备开始识别流量时，会首先对流量进行高层协议分析，除了基本的 TCP/UDP 协议，还支持 HTTP、FTP、SMTP、POP3、IMAP 等 20 多种协议解析，对于不同的协议可以分析出不同的信息，例如获取报文的 IP 地址、端口号，对于 HTTP 协议，可以获取请求的 URL，请求头部的 Host 字段信息等。此时，对于 SSL 加密流量，在识别前需要进行 SSL 解密工作。

2.3.5.1 扫描识别

进行初步的协议识别后，对于流量会进行进一步的分析，主要手段有 DPI（深度报文检测）和 DFI（深度流检测）两种。其中 DPI 方面主要是进行 Payload 的扫描识别，通过 AC 算法、正则匹配等多种方法对静态报文进行内容解析，提取报文中的关键字或其他需要的信息；而 DFI 方面，提供跨报文识别的解决方案（例如依据包长序列识别迅雷）和流量关联识别（例如通过 FTP 控制通道关联数据通道）。

2.3.5.2 关键信息

当完成应用识别工作以后 ,弘积上网行为安全审计设备基于不同的应用类型去匹配应用特征库 ,使用各类技术手段对获取的信息进行解码和还原 ,从而能够获取到关键信息的明文，并将审计结果存储到数据库中。

2.3.5.3 关键信息审计

近年来 ,一方面随着国家为了净化互联网环境 ,逐步建立对互联网行业发证的市场规范，监管力度不断增强，另一方面，组织出于自身信息安全保护的需求如防止信息资产泄密，预防舆论风险，保留安全事件的相关证据，已经管理上的要求，如考核员工的网络工作效率、分析网络应用情况、提供管理依据等，对于行为记录方案的需求日益明确。

内网用户的所有上网行为 AC 都能够记录以满足公安部 82 号令的要求。弘积上网行为安全审计 可针对不 同用户(组)进行差异化的行为记录和审计，包括网页访问行为、网络发帖、邮件 Email、IM 聊天内容、文件传输、游戏行为、炒股行为、在线影音、P2P 下载等行为，并且包含该行为 的详细信息等。

近年来信息防泄密方案备受组织管理员关注，内网员工无意或有意将组织机密信息泄露 到互联网甚至竞争对手，或向论坛 BBS 发布不负责的言论、网络造谣等，将给组织带来泄 密和法律风险。弘积上网行为安全审计不仅能基于关键字过滤、记录员工通过 Mail（包括 Webmail）、BBS、 Blog、QQ 空间等发布的网络言论，还日志记录功能。

对于使用 HTTP、FTP、mail 等方式传送文件所引发的风险（如将研发部的核心代码发 送出去），首先 弘积上网行为安全审计可以禁止用户使用 HTTP、FTP 上传下载指定类型的文件，对于上传的 文件弘积上网行为安全审计 也可以全面记录文件内容，做到有据可

查。而外发 Email 潜在的泄密风险通过 弘积上网行为安全审计 的邮件延迟审计（Postponed Sending after Audit，PSA）技术，根据管理员预设条件， 将潜在的泄密邮件先拦截，经人工审核后再发送，保障组织信息资产安全。但存心的泄密者 通常会更改文件后缀名、删除后缀名、压缩、加密等，再通过 Email 外发、或通过 HTTP、 FTP 上传，弘积上网行为安全审计 对以上行为同样可以识别并实时记录审计日志。

在移动互联网的兴起下，移动 APP 的使用已经越来越普遍，因此，公共社交类移动应用将成为发布不实言论、造谣诽谤等的重灾区。弘积上网行为安全审计紧随时代步伐，针对移动端的新闻评论 类（腾讯新闻、网易新闻、新浪新闻等）、微博（新浪微博等）、论坛类（百度贴吧、天涯社 区、新浪论坛、搜狐社区等）APP 进行内容审计，保护移动互联网时代的网络内容安全。

2.3.6 终端识别

弘积上网行为安全审计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。

2.3.6.1 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。

弘积上网行为安全审计识别用户系统、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。

2.3.6.2 **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

2.3.6.3 **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。

2.3.6.4 **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。

2.3.6.5 支持的设备列表

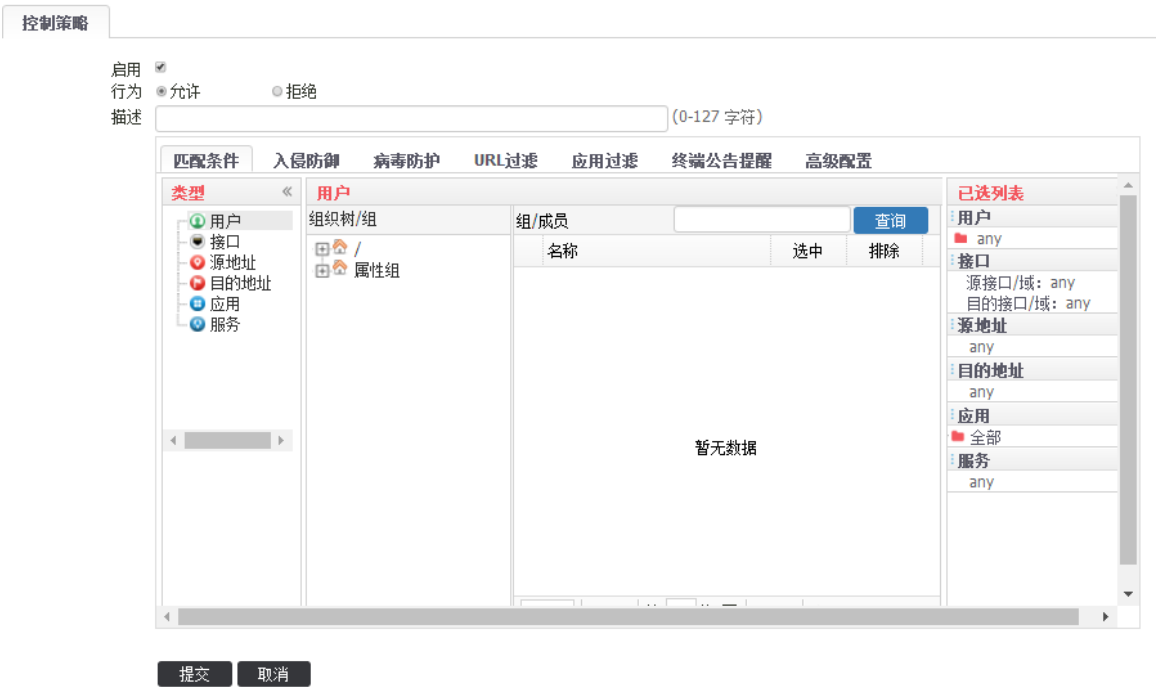
弘积上网行为安全审计的终端识别和审计适用于市场上主流的设备：Windows、iPhone、iPad、Android 等。

2.3.7 访问策略

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，而弘积上网行为安全审计的出现让访问控制变得简单，基于 7 元组以及时间和终端维度的访问控制策略，能有效的控制自然人、应用的访问控制。

2.3.7.1 精细化控制策略

弘积上网行为安全审计采用精细化控制策略，管理员只需要通过一条策略便可完成对源接口、源地址、用户、目的接口、目的地址、应用、服务、时间、终端类型等维度的匹配，并针对入侵防御、病毒防护、应用过滤、URL 过滤、终端公告提醒等进行统一管控，使用方便，维护简单。



2.3.7.2 精细化管控

弘积上网行为安全审计内置千万级 URL 库 ,拥有近 4500+种主流网络应用及应用行为，涵盖即时通讯、P2P 软件、网络游戏、电子商务、办公软件等 29 类主流应用类型。满足精细化应用和网站控制需求，企业内网管理更加灵活精准和高效。

最新应用分类：

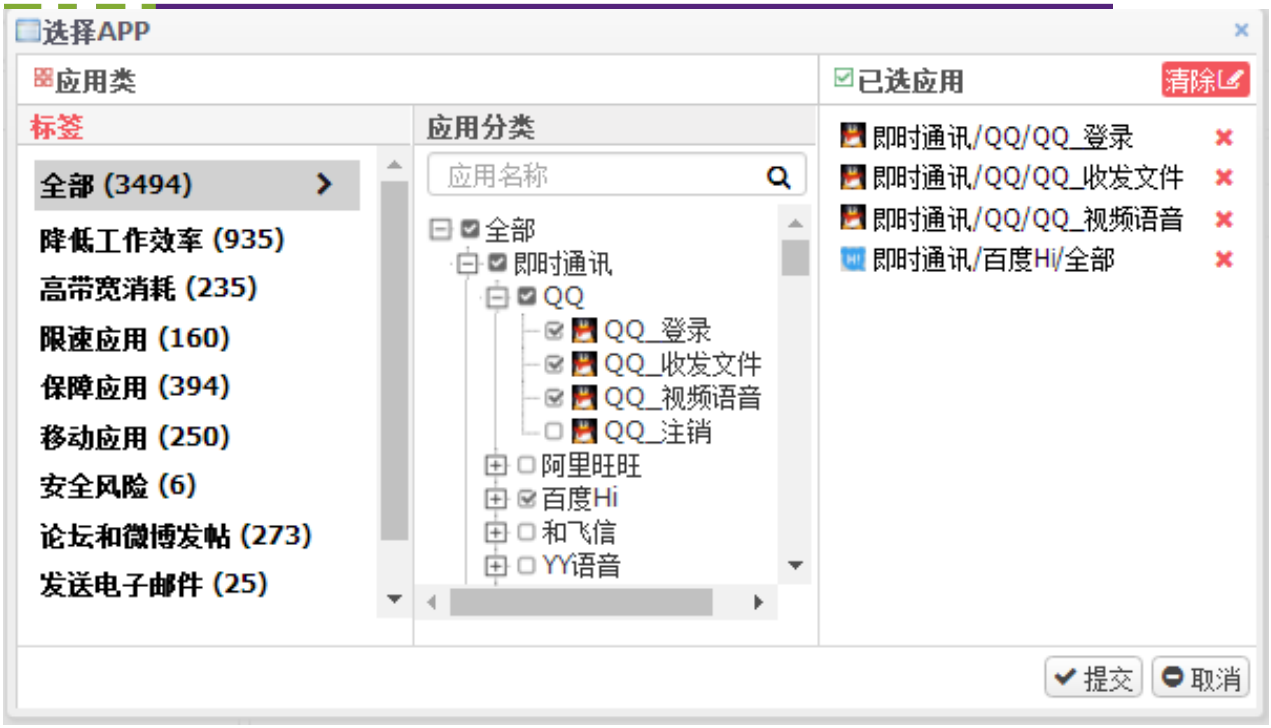
- ✓ 即时通讯
- ✓ P2P 软件
- ✓ P2P 流媒体
- ✓ 其他流媒体
- ✓ 金融登录
- ✓ 金融行情
- ✓ 金融交易
- ✓ 网络游戏
- ✓ 文件传输
- ✓ 云端存储
- ✓ 搜索引擎
- ✓ 网络社区

- ✓ 微博
- ✓ 门户网站
- ✓ 数据库
- ✓ 电子商务
- ✓ 网上银行
- ✓ 网络协议
- ✓ 电子邮件
- ✓ 远程控制
- ✓ 木马控制

- 应用管控
  - ✓ 生活服务
  - ✓ 招聘咨询
  - ✓ 文学咨询
  - ✓ 网络代理
  - ✓ 办公软件
  - ✓ 软件更新
  - ✓ P2P 信贷
  - ✓ 其他类

弘积上网行为安全审计通过对数据包的深入解析，精细化获取应用及应用的相关行为，完成网络实时应用和系统应用的应用指纹匹配。此外针对应用指纹模糊的应用系统通过管理分析应用的行为轨迹通过应用行为完成指纹模糊应用的精准识别。依附引擎对应用的精准识别实现应用的精细化控制。并完成相关应用的日志记录。

精细化为的应用分类和应用行为通过层次结构分明的树形结构完成展示，供管理员用户策略引用。



传统的应用控制之外针对邮件控制；Web 关键字控制；虚拟账号控制同样完成精细化，标准化的梳理。

邮件的控制一直是上网行为安全审计标榜的核心功能。功能的精细化和直观展现直接影响产品的市场反馈。针对邮件的精细化控制我们弘积上网行为安全审计从如下角度完成标准化：

- 发件人
- 收件人
- 邮件标题和内容
- 邮件大小
- 邮件附件个数

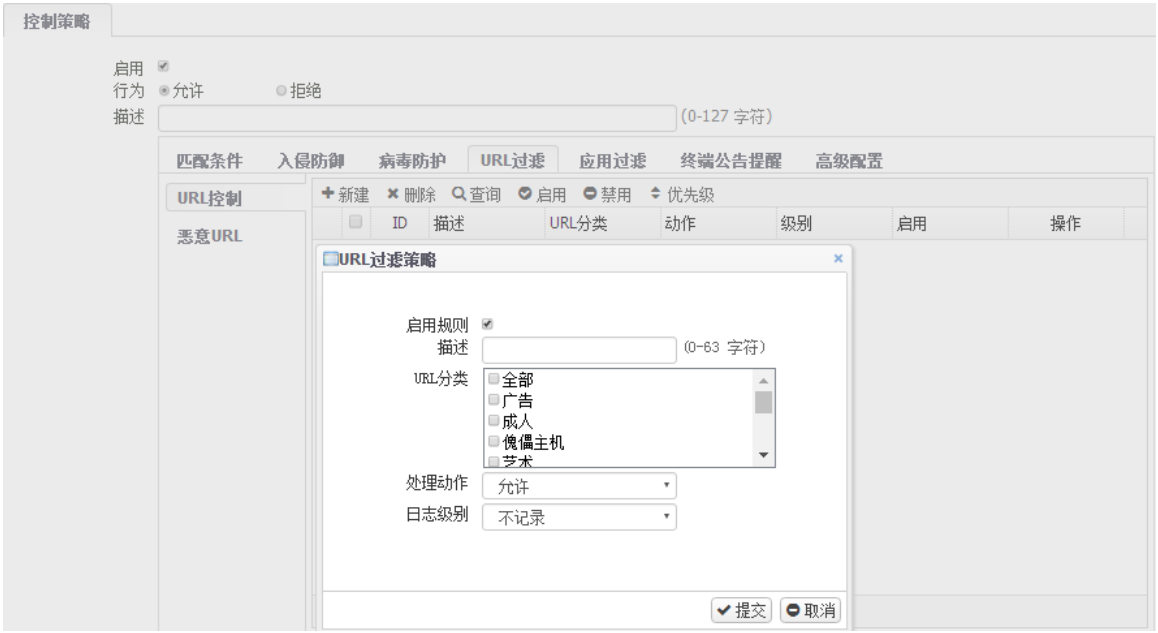
全维度覆盖邮件的所有模块。针对发件人和收件支持黑名单或者白名单的便捷控制。满足各种控制需求。

Web 关键控制主要解决市场常见的信息泄露、行为审计、舆论评论等相关问题。弘积上网行为安全审计采用深度分析引擎和 SSL 解密引擎完成对加密和非加密数据的深度分析。

虚拟账号控制虽然是行为管理的小众场景，但是随着网络时代的发展及国家针对行业的规范化。虚拟账号作为用户身份的标识需求也越发重要。对于弘积上网行为安全审计的理念是以用户维度触发控制记录用户的行为。虚拟账号作为用户的标识同样需要精细化控制。

- URL 管控

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。



- 终端公告提醒

弘积上网行为安全审计主要完成对用户的行为管控，管控的代价势必会造成部分网络阻断。如果静默的方式控制网络，终端用户体验极差。控制的同时合理提示终端用户才能保证产品更好的适应市场发展。

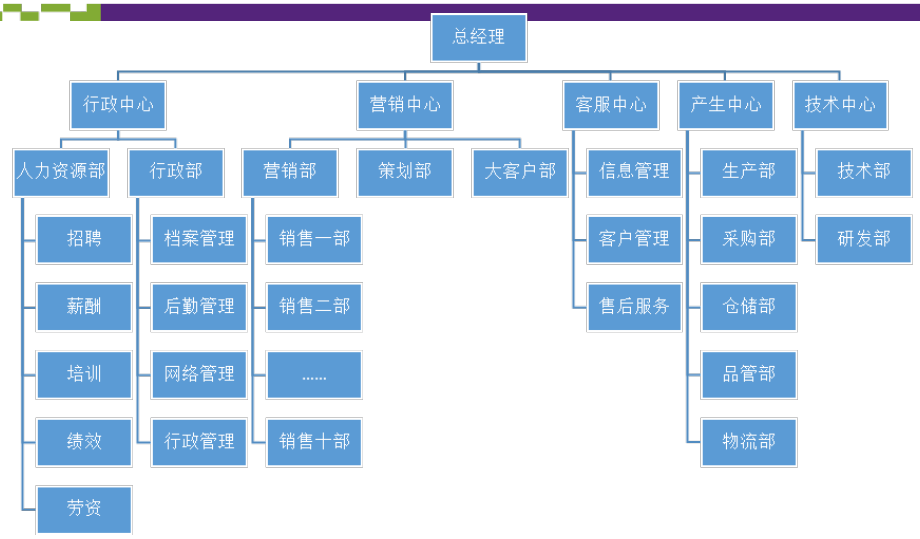
因此弘积上网行为安全审计完成终端公告提示功能，且提示内容支持管理员自定义。这样不仅解决了用户网络控制的困扰且进一步提升产品的用户体验。

2.3.8 流量管理

弘积上网行为安全审计使用了 DPI 和 DFI 融合应用识别技术，

2.3.8.1 4 级通道管控

随着企业规模的不断扩大，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，为此弘积上网行为安全审计系列提出了 4 级流控概念，可将物理线路划分为若干虚拟线路和流控通道，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	-	广东省邮	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	

2.3.8.2 弹性带宽分配

弘积上网行为安全审计弹性带宽管理，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。此特性避免了带宽浪费，实现价值最大化。

2.3.8.3 流量、时长限额

用户体验至上的服务理念趋势下，企业为用户提供更灵活和细致的服务，已达到用户差分服务的效果。例如银行网点中，铜卡用户可免费上网 3 小时，银卡用户可免费上网 5 小时，金卡用户不限时上网。单纯的流控策略是无法满足企业的管理需求。

弘积上网行为安全审计提供流量和在线时长限额的功能。通过预设用户的流量额度或者在线时长的阀值，设备统计该用户的对应参数，当对应参数超过设置阀值，设备立即对该用户进行惩罚，惩罚方式可选择禁止上网或流量限速。

弘积上网行为安全审计可提供极为强大的管理网络流量的方法和手段，解决用户应用场景的流控细致化、差异化需求。

2.3.8.4 每 IP 或用户限速

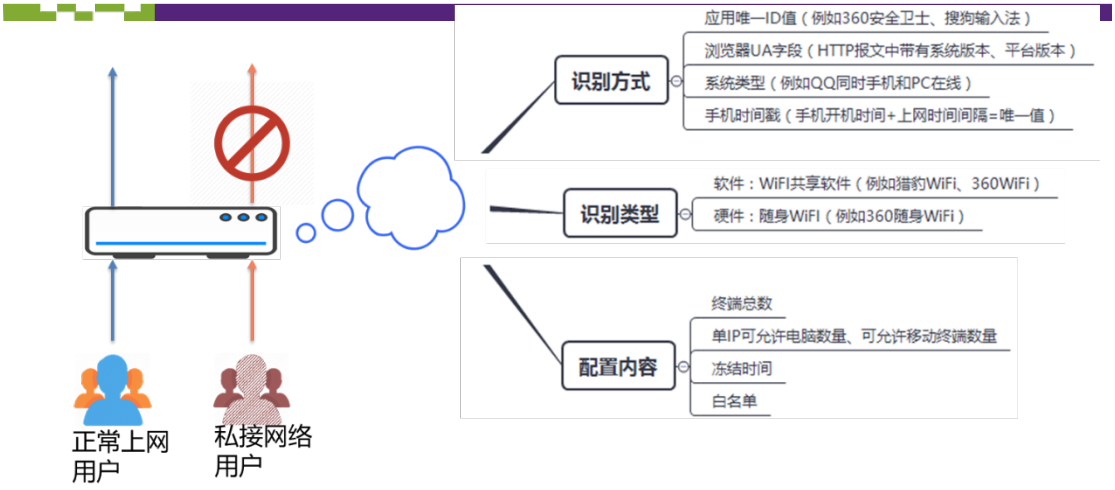
弘积上网行为安全审计采用了自动均分带宽，当在某个通道中只有一个用户使用时，该用户可以使用全部的带宽，如果有更多用户使用该通道时，管理员可设置将带宽按 IP 数量或用户数量均分，提升用户上网体验。

2.3.8.5 流控策略白名单

网络管理过程中，重要来宾和企业重要人员往往是不希望受流控策略的限制，弘积上网行为安全审计根据用户需求，增加了流控策略白名单功能，白名单 IP 和用户将不受弘积上网行为安全审计任何流量策略的限制，保障管理更加人性化。

2.3.9 防私接路由

上网用户私接 WiFi 或路由器行为会造成无法校验用户身份、安全性能难以保障、占用额外带宽资源等问题。弘积上网行为安全审计能够快速识别“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；同时弘积上网行为安全审计支持同步和展示认证用户信息，支持同步 PPPOE 账号等认证服务器账号信息。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。



2.3.10 安全管理

2.3.10.1 会话管理

会话监控、会话控制功能是专业化管理内网必不可少的功能。弘积上网行为安全审计可对当前设备的会话进行监控，管理员可查看会话的发起用户、源目地址、端口、协议、策略、存在时间和超时时间等，具有完备的状态检测表追踪连接会话状态；弘积上网行为安全审计支持对当前所有会话进行峰值统计，方便管理员快速筛选内网异常用户和 IP，可帮助管理快速定位网络故障；管理员支持针对全局基于 IP 进行并发会话和新建会话的限制，保障内网所有访问行为均在正常数值范围内，确保内网安全。

2.3.10.2 黑名单

弘积上网行为安全审计支持黑名单设置并支持黑名单时长设定，用户上网行为中触发防攻击规则后源地址自动进入黑名单。有效提升了用户网络安全性

2.3.10.3 攻击防护

当受到攻击时，伴随而来的会出现网络异常情形发生，网络异常大概可分为以下三种：

- 通信协议异常

例如由外界网络流入大量过长的 IP 数据包、大量的 IP 碎片数据包、异常的 TCP 通信协议连机状态、被截断的 IP 数据包、无法重组的 IP 数据包等。

- IP/Port 的扫描异常

通过 IP 扫瞄，黑客得以窥知目的端内网络结构和情形；通过 Port 扫描，黑客可以得知目标主机已开启的服务端口。

- 网络流量异常

例如突然产生大量的 TCP SYN、TCP、UDP、ICMP、IGMP 等数据包，占据正常网络使用带宽。

当上述攻击数据包发起时，经过改造的恶意数据包可能会造成企业内部网络系统死机无法对外提供正常的服务；IP/Port 扫瞄的行为将让企业内部的网络架构轻易被黑客得知；大量的异常流量数据包也可能造成企业核心路由器、交换机等因承载过重而死机。

弘积上网行为安全审计内置异常包攻击防御模块，可以检测各项偏离预期的网络行为。依据 RFC 标准规范制作通信协议异常检测模块，可以阻止不符合标准通信协议规范的数据包。支持网络流量异常检测，不单只使用计数的方式，还使用专门的统计算法，可以准确地检测网络流量的异常情形。

- 支持 ARP 防欺骗、支持 IP、MAC 地址绑定。
- 支持 ARP Flood 攻击防护、支持基于接口的 ARP 学习控制。
- 支持 Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP 选项、IP Spoof、Jolt2 等异常包攻击的防御。
- 支持基于 IPv6 的 Winnuke、Land-Base、TCP flag、Fraggle、IP Spoof 等异常包攻击的防御。
- 支持基于接口的端口扫描防护和 IP 扫描防护。
- 支持 SYN flood、UDP flood、ICMP flood、DNS flood 攻击防护，支持自定义阈值。

2.3.11 统计报表

弘积上网行为安全审计系列支持实时的数据统计功能，对用户网络行为进行记录与分析。对于日志的留存与分析，即是对国家法律法规的遵从，也是真正管理好企业员工上网，有效利用网络资源的需要。正对用户上网行为以及相关内容查询统计，能够对用户的网络活动进行较长时间的回溯与反查，版主管理员全面了解网络的使用情况，为改进网络管理提供详实准确的依据。

2.3.11.1 实时统计

弘积上网行为安全审计系列内置多套用户行为管理统计汇总模板。管理员可以根据时间维度，全方位查询统计用户，应用等相关上网行为数据。其内容涵盖用户上网行为次数统计、邮件审计统计、IM 审计统计、关键字排名统计、恶意 URL 统计等相关数据统计。为管理员用户提供不同角度的统计报告。

弘积上网行为安全审计系列支持实时的数据统计功能，对用户网络行为进行记录与分析。对于日志的留存与分析，即是对国家法律法规的遵从，也是真正管理好企业员工上网，有效利用网络资源的需要。正对用户上网行为以及相关内容查询统计，能够对用户的网络活动进行较长时间的回溯与反查，版主管理员全面了解网络的使用情况，为改进网络管理提供详实准确的依据。

2.3.11.2 报表订阅

弘积上网行为安全审计系列除了提供实时的统计报表功能之外，还为用户提供报表订阅功能，系统内容多套不同的报表模板，且管理员可以根据需求自定义报表内容，为不同行业用户提供最大程度的满足。系统内置的报表订阅功能支持以天、周、月以及自定义时间范围等多种时间维度的报表统计。统计生成之后的报表支持通过邮箱，ftp 等多种方式发送和上传到第三方，且设备针对历史报表也预留一定的存储空间。从而保证报表数据不会因为外置设备异常导致数据丢失。

2.4 营销特性

2.4.1 用户行为轨迹

弘积上网行为安全审计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，将用户的虚拟身份和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，有利于营销人员收集上网用户的网络账号和行为习惯，通过大数据分析实现精准营销推广。实现网络资源的合理利用的同时，提升数据价值。

2.4.2 用户标签

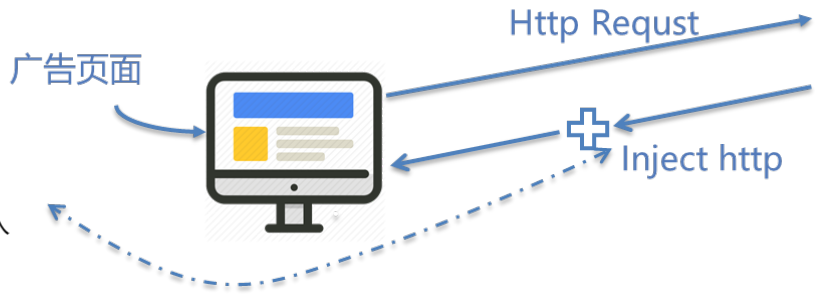
互联网时代中，用户的兴趣点千差万别，如何从用户的兴趣点切入，增加用户粘性，这是企业近年来关注的问题。弘积上网行为安全审计可根据用户审计信息分析，如用户一天网站访问中，购物网站比例高于多少即给用户打上“购物”标签，通过预留的 Port 服务器 API 接口，将用户标签同步至 Port 服务器。用户认证时 Port 服务器推送预定义的 Port 页面，可实现定向营销和差分服务，有效的增加用户粘性，提供更多个性化的需求场景。

2.4.3 多广告推送

企业于投放通知或营销信息时，需向用户快速的下发消息，传统的消息传播方式速度慢且成本较高，非常不适用。弘积上网行为安全审计提供多广告推送功能，可基于五元组维度向用户访问的网页中插入弹窗页面，支持同时弹送 4 个页面，且弹送位置可自定义，具备极高的灵活性，复用已有网络线路，节省成本。在营销场景中，弘积上网行为安全审计多广告推送功能极具优势。

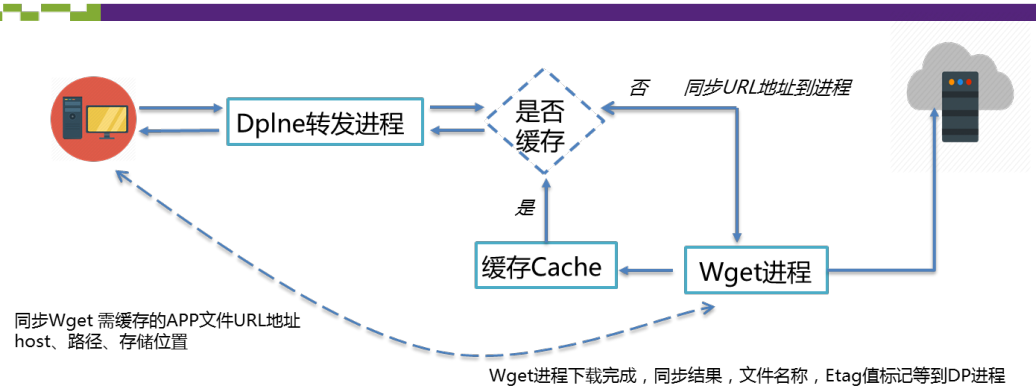
流量劫持注入条件：

- HTTP 200 OK 响应报文
- Request Method为GET或POST
- Content-Type: text/html
- 多条件且关系执行HTML末尾注入



2.4.4 应用缓存

弘积上网行为安全审计创新的将 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；具备精确缓存、模糊缓存特性，可解决 Android 平台升级 URL 变更频繁问题；支持动态缓存，自动更新 APP，无需管理员频繁手动上传，业界技术领先；弘积上网行为安全审计应用缓存功能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。



2.5 合规特性

2.5.1 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，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，弘积上网行为安全审计提供了 SSL 审计功能，弘积上网行为安全审计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，包括 Webmail 和客户端 Mail 等行为进行识别。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。

- 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。

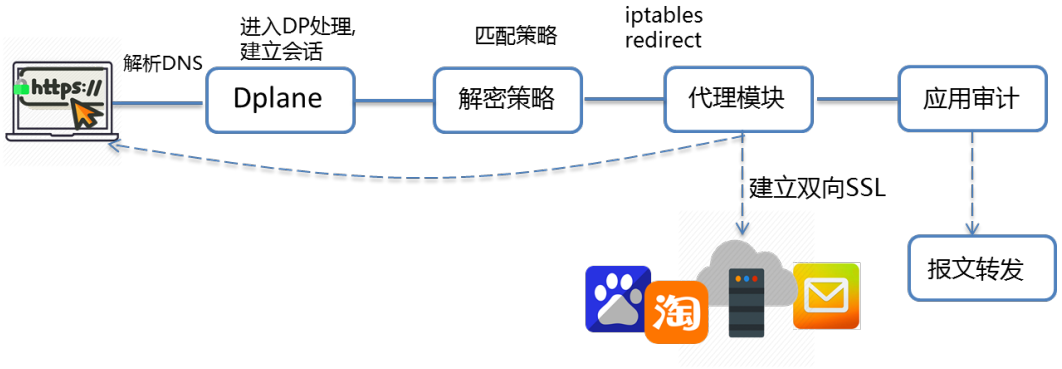
- 解密策略

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。

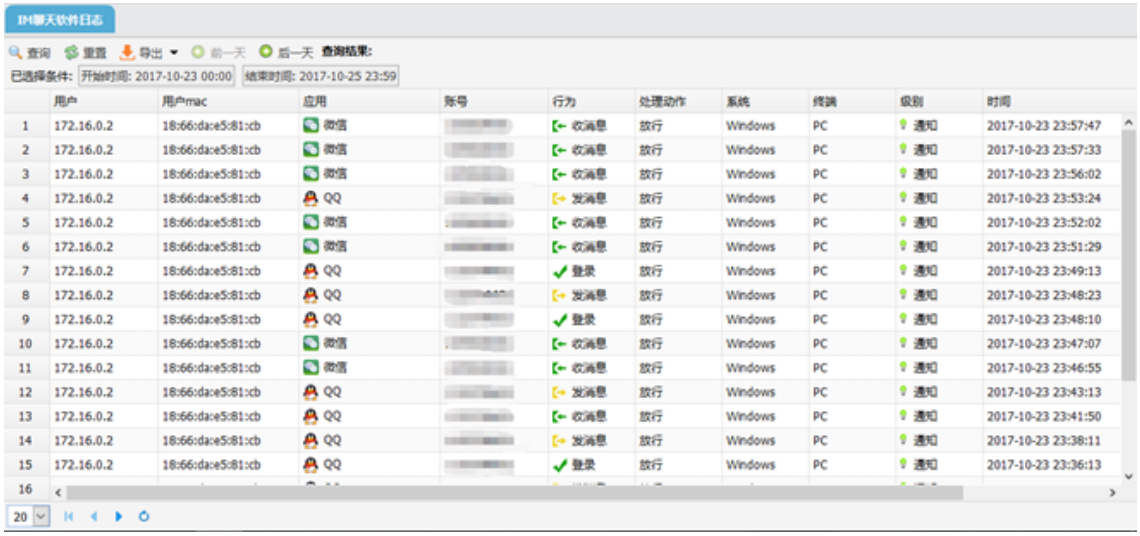
网页版邮箱需匹配第四个维度-域名，该域名系统内置。



2.5.2 清晰事后审计

弘积上网行为安全审计支持详细、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，可满足公安部要求的上网日志留存 6 个月的要求；

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，弘积上网行为安全审计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。



2.5.3 审计日志导出

随着国家净化互联网环境的趋势，对于网络监管力度不断增加；并且企业为了预防关键信息泄露，提升员工工作效率，对上网行为审计日志的需求愈加强烈。

弘积上网行为安全审计支持按照“今天、近三天、近一周、近一月、近三月”等时间维度导出日志，定期留存日志，实现对历史记录有据可查，保障内网信息安全。

2.5.4 无线非经

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。

弘积上网行为安全审计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。弘积上网行为安全审计支持任子行、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。

2.6 运维特性

2.6.1 U 盘零配置上线

企业的网络运维人员流动性较大，技术水平层次不齐，设备上线时，往往会面临较多技术问题，实施周期相对较长。管理员对不同局点的设备完成预配置，保存在 U 盘中（保存在 U 盘中的配置文件经过加密），开局人员拿着此 U 盘插入开局的设备，设备通过序列号获取 U 盘内的配置内容，完成设备的零配置上线工作。方便了设备的快速上线，极大的缩短了实施周期。

2.6.2 多配置切换

总分型连锁场景中，网络运维力量相对较弱，灾备情况时，用户的关键业务无法快速切换，正常业务无法得到保障。弘积上网行为安全审计支持通过命令行或者预留的 API 接口切换配置文件，设备的业务数据和访问规则快速切换，保障网络的正常可用。

2.6.3 高可靠性

弘积上网行为安全审计具备高可靠性，具体体现在软件和硬件两个方面。

2.6.2.1 软件部分

- 接口：接口支持最多配置 200 个从属 IP，保障接口有充足的地址使用；
- 路由：ISP 路由、策略路由、负载均衡等路由，保障流量按需分流；
- 策略：按需分配上网权限，保障网络正常运行；
- 日志：攻击行为有迹可查；
- HA：主主、主备模式保证网络持续运行，支持 VPN 级别的 HA 功能。弘积上网行为安全审计除了支持主主、主备模式功能，同步配置、运行状态、会话、用户上线状态、特征库等内容之外，能够同步 IPsec VPN 状态。VPN 对于电信级业务来说是命脉，如果普通设备的 VPN 断开重连，按照协议标准，算上 DPD 超时和 IKE 建立的时间，估计在 100 秒到 120 秒，其中的时间成本是企业无法承担的。弘积上网行为安全审计完美的解决了这个问题，主备设备同步 VPN 的状态，主备切换时，零丢包零中断，保障用户的关键业务不中断，极大的避免了企业的损失；
- 配置备份：设备的关键配置自定义备份，支持多配置切换，可保障设备快速恢复；

2.6.2.2 硬件部分

- 接口：接口数量丰富；
- 电源：提供冗余电源；
- 风扇：提供冗余风扇；
- Bypass：支持硬件 Bypass

2.6.4 服务质量管理

网站和关键服务器的链路质量是企业重点关注的问题之一，如何衡量服务器提供的业务质量，是网络维护人员的值得思考的问题。

弘积上网行为安全审计的服务质量探测，使用 PING、DNS、TCP 等探测协议，检测目标地址的成功率、延时等数据，帮忙网管及时的发现服务质量较差的服务，从整体上展示关键服务的状态，达到优化整体网络，提升关键业务的服务质量。

2.6.5 端口镜像

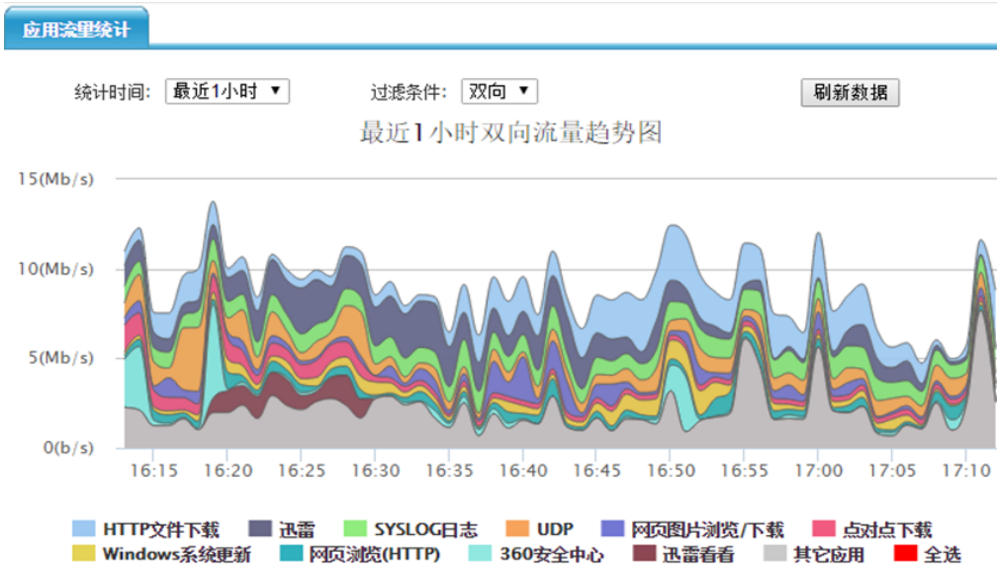
弘积上网行为安全审计在审计所经过流量的同时，可提供端口镜像功能，支持将对应接口按照入流量、出流量或双向流量等规则类型进行流量镜像，提供流量分析功能，帮忙网络管理员提供运维工具，并节省一台交换机的成本。

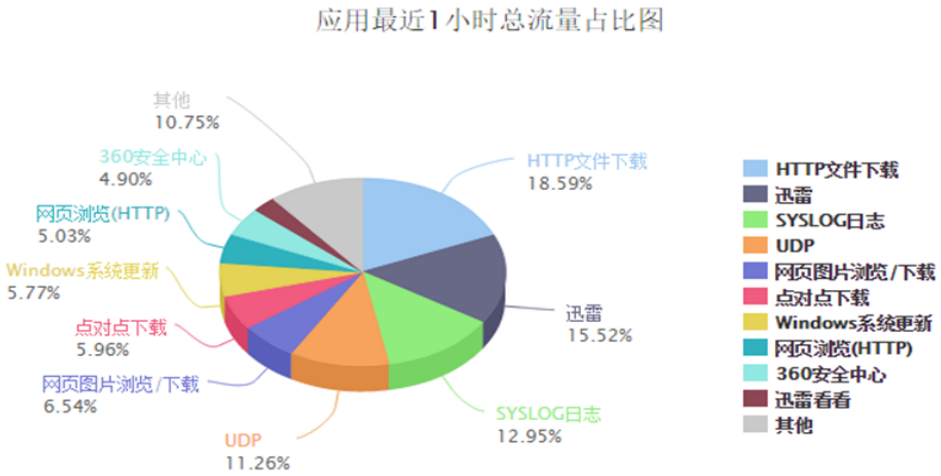
2.6.6 管理端口自定义

当前较多网络设备使用默认端口和默认密码， 极易被黑客攻击，造成经济损失。弘积上网行为安全审计提供管理端口自定义功能，管理员可配置非常用端口号，增强设备的安全性，避免经济损失。

2.6.7 应用和用户流量统计

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。


应用流量统计
统计时间: 最近1小时
过滤条件: 双向
刷新数据
最近1小时双向流量趋势图
15(Mb/s)
10(Mb/s)
5(Mb/s)
0(b/s)
16:15 16:20 16:25 16:30 16:35 16:40 16:45 16:50 16:55 17:00 17:05 17:10
HTTP文件下载 迅雷 SYSLOG日志 UDP 网页图片浏览/下载 点对点下载
Windows系统更新 网页浏览(HTTP) 360安全中心 迅雷看看 其它应用 全选


应用最近1小时总流量占比图
其他 10.75%
360安全中心 4.90%
网页浏览(HTTP) 5.03%
Windows系统更新 5.77%
点对点下载 5.96%
网页图片浏览/下载 6.54%
UDP 11.26%
SYSLOG日志 12.95%
迅雷 15.52%
HTTP文件下载 18.59%
HTTP文件下载
迅雷
SYSLOG日志
UDP
网页图片浏览/下载
点对点下载
Windows系统更新
网页浏览(HTTP)
360安全中心
迅雷看看
其他

2.6.8 业务告警

弘积上网行为安全审计支持业务告警功能，可针对 CPU、内存、会话、整机流量和 IPsecVPN 连接断开等关键设备内容进行告警，提供页面弹窗和邮件告警提醒，快速定位故障点，及时向网络管理提供设备状态，助力运维。

2.6.9 管理员外部认证

弘积上网行为安全审计对于管理比较严格的行业支持管理员外部存储、认证。可直接对接 AD 和 Radius 系统。提供系统健康探测功能。如果服务器故障可通过智能启动本地认证方式、避免设备失联。

2.6.10 集中管理与数据分析系统

弘积上网行为安全审计日志分析与管理平台是提供对弘积上网行为安全审计的集中监控、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。利用日志分析与管理平台，管理员可以高效地管理各弘积上网行为安全审计设备，全面掌握网络的整体安全状况。

2.6.10.1 采用高性能数据存储和查询

弘积上网行为安全审计日志分析与管理平台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。

弘积上网行为安全审计日志分析与管理平台支持 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日志分析与管理平台前日志存储 1 个月产生 500G 数据，而采用弘积上网行为安全审计日志分析与管理平台后，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。

2.6.10.2 **深层次数据挖据分析**

弘积上网行为安全审计日志分析与管理平台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。

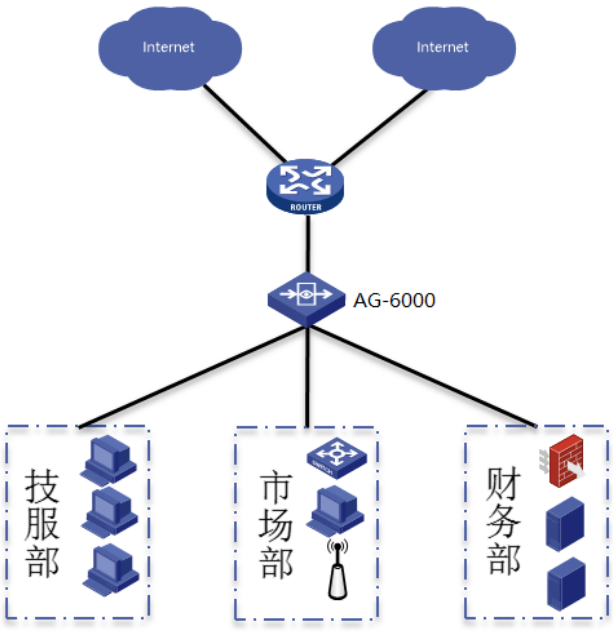
数据仓库中包含 ETL、数据模型、信息展现等主要关键技术。ETL 是数据抽取（Extract）、清洗（Cleaning）、转换（Transform）、装载（Load）的过程。它是构建数据仓库的重要一环，用户从数据源

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。

3 典型组网应用

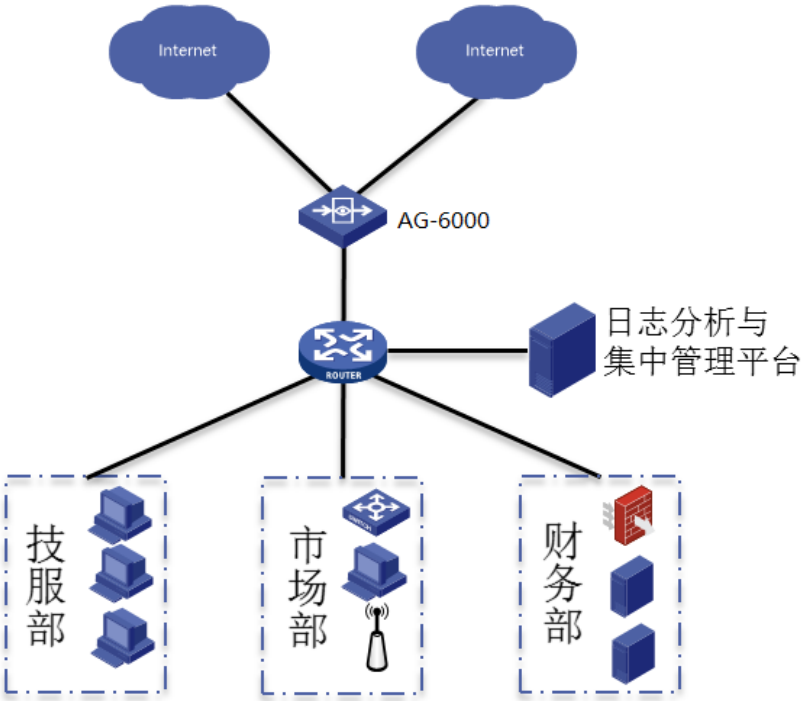
3.1 透明部署

- 适用于数据中心机房，可灵活的以串行路由或者透明方式部署于数据中心机房出口，根据实际网络环境署简单；
- 提供身份认证功能，验证上网用户身份合法性；
- 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；
- 支持设备本地日志记录，日志也可发送到集中管理和数据分析中心处理，并可进行数据分析。



3.2 路由部署

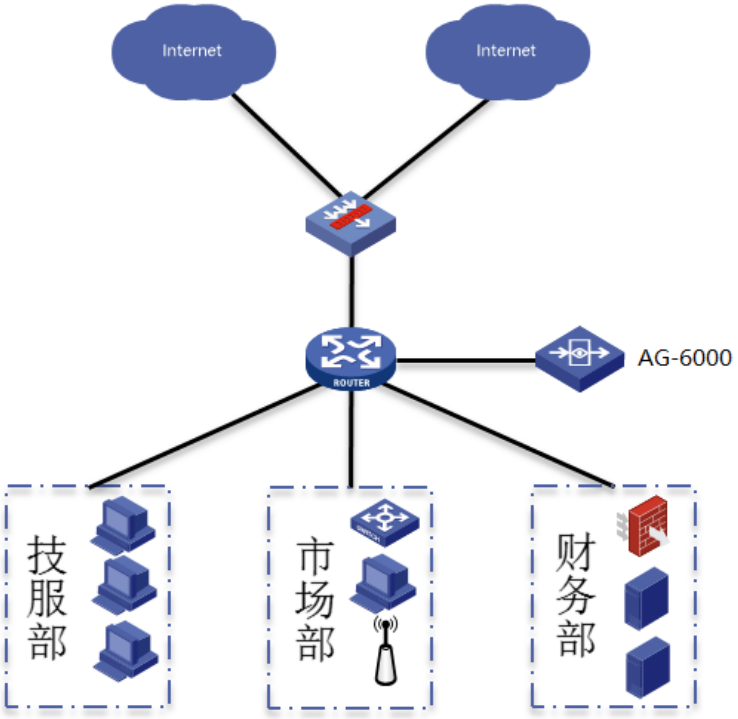
- 适用于大中型企业用户，以网关方式在线部署于网络出口；
- 提供诸如 NAT、负载均衡等出口特性；
- 对网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等各种应用进行监控和管理，保障关键应用和服务的带宽；
- 支持 VPN/MPLS/ VLAN/PPPoE 等复杂网络环境；
- 支持设备本地日志记录和集中分析处理，可多台分布式部署统一管理。



3.3 旁路部署

- 适用于不改变网络拓扑，仅做行为审计的场景，一般部署于核心层；
- 针对用户上网行为进行分析和审计；

- 提供日志记录、日志导出功能。



4 功能列表

一级 SPEC	二级 SPEC	三级 SPEC	四级 SPEC
网络功能	部署模式	旁路	单接口监听交换机镜像流量
		串行	支持透明、路由、混合（透明+路由）、多组桥、多口桥
		混合	支持旁路和串行混合部署
	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
	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	支持基于路由权重的多链路负载均衡
		策略路由	5 元组策略路由+应用+时间
		ISP 路由	内置电信、联通、移动、教育网 ISP 信息，可自定义 ISP 信息

		RIP	支持 v1、v2
		OSPF	支持缺省路由发布、路由重发布
	NAT	通用功能	支持源 NAT、目的 NAT、静态 NAT
			支持一键 NAT 回流（双向 nat）
		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
	会话限制	规则管理	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）
	地址探测	接口探测	支持 PING、TCP、DNS 地址监控条目
		地址探测组	支持多个地址探测从属组关系
		路由探测	支持探测路由以确保路由有效性
	链路负载均衡	链路负载均衡	支持基于权重、优先级的七元组链路负载均衡
			负载均衡接口支持健康探测
	服务器负载均衡	服务器负载均衡	支持基于源地址散列+权重的服务器负载均衡
			支持服务器组服务或服务器健康状态的探测
	DDNS	DDNS	支持花生壳 ddns 客户端以及域名 IP 绑定
网络优化	APP 动态缓存	APP 动态缓存	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
	应用缓存	应用缓存	支持文件的应用缓存，支持文件名模糊匹配的文件缓存
	服务质量管理	服务质量管理	支持 PING、TCP、DNS 探测
			支持自定义间隔时间探测
虚拟路由器	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
入侵防御	入侵防御	入侵防御	支持基于源、目的、规则集的入侵检测
			支持入侵防御高阶告警。支持 FTP 和邮件方式
		特征库	系统定义超过 3000 条规则 ,包含 Backdoor ,bufferoverflow，dosddos，im，p2p，vulnerability，scan，webcgi，worm，game。
病毒防护	病毒防护	病毒防护	查杀邮件正文/附件、网页及下载文件中包含的病毒
		病毒防护	支持启发式扫描查杀未知病毒
安全防护	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
	扫描防护	通用	基于接口的配置，支持自动加入黑名单
		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	支持 ARP 学习与主动保护，防 ARP Flood 攻击
		ARP 学习控制	基于接口的 ARP 学习控制
	Flood 防护	支持类型	SYNFlood、UDPFlood、ICMPFlood、DNSFlood
Web 防护	基础配置	策略配置	支持基于源地址、目的地址、服务端口的策略匹配
		安全配置	支持防护规则；精细访问控制；防盗链；CSRF 攻击防护；CC 攻击防护；应用隐藏；网页防篡改。
	安全防护	规则防护	内置 http 协议检查；通用攻击；SQL 注入攻击等 11 种规则防护
		精细访问控制规则	支持管理员自定特征匹配字段完成精细化控制
		防盗链	支持针对全站；特定 URL；特定文件类型等防护
		CSRF	支持针对特定 URL 特定控制访问来源
		CC 攻击	支持针对全站和特定 URL 实时监控防护，允许管理员配置触发条件
		应用隐藏	支持管理员配置特定字段的应用隐藏
风险扫描	端口扫描	扫描任务	支持管理员配置特定资源的端口扫描任务，提前发现潜在风险
		扫描结果	扫描的结果展示，且支持管理员根据扫描结果操作
	弱密码扫描	扫描任务	支持管理员创建弱密码扫描任务
		扫描结果	扫描的结果展示，且支持管理员根据扫描结果操作
		字典管理	系统内置密码字典；且支持管理员导入密码字典
流量管理	通用功能	配置管理	增删改
	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
	排除策略	排除策略	支持用户、地址排除
	限额策略	限额策略	支持基于时长、流量的限额策略
			支持超出限额阈值时进行阻断，流控
解密策略	https 网站解密	https 网站解密	支持基于策略的 https 网站解密
			支持自定义 https 网站解密
			支持预定义 https 网站解密
	ssl 邮箱	ssl 邮箱解	支持 ssl 加密网页版邮箱的解密

	解密	密	支持 ssl 加密客户端版邮箱的解密
防共享上网	防共享上网	防共享上网	支持用户共享网络监测
			支持阻断和限速两种惩罚方式
			支持共享网络用户终端数阀值配置，支持不同终端单独配置
访问控制	IPv4 策略	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、服务以及时间和终端类型
			支持应用控制，URL 过滤、终端公告推送的策略动作
			基于策略的长连接（老化时间）
	IPv6 策略	配置管理	支持用户和应用均为任意的 7 元组策略
上网行为控制与审计	应用控制	应用控制	支持根据应用配置应用控制策略
		邮件控制	支持针对发件人；收件人；标题&内容；邮件大小；附件个数控制
		web 关键字控制	支持搜索引擎；http 上传；http 页面内容的关键字控制
		虚拟账号	支持针对 QQ 虚拟账号的黑白名单控制
		URL 控制	支持预定义和自定义 URL 分类过滤
		终端公告	支持根据策略的终端公告内容推送
	应用审计	http 审计	支持网页访问；网络社区；网页搜索；http 外发文件；http 文件下载的审计
		邮件审计	支持发邮件；收邮件；web 邮件的收发审计
		即时通讯	支持 QQ 客户端；微信客户端；网页 QQ；网页微信；移动飞信等聊天内容审计
		基础协议	支持 FTP；TFTP；TELNET 基础网络协议账号，命令等内容的审计
		娱乐股票	支持股票娱乐账号和评论的审计
		网络应用	支持其他大类网络应用的审计
统计报表	报表管理	报表管理	支持新建以日、周、月为单位的报表任务，以及单次报表，报表任务支持启用、禁用
			支持多种模板的报表，支持管理员自定义报表模板
			支持通过邮件和 ftp 的方式外发报表
			报表支持 pdf 和 html 两种格式
			订阅项目支持：设备维度；行为管理数据统计维度；网络质量维度；网络安全维度
		历史报表	报表任务支持完成之后删除本地历史报表，也支持本地保留历史报表
			历史报表的空间支持自定义

	数据统计	统计	支持基于用户上网行为次数；用户访问网站；用户邮件审计；即时通讯等多种维度的数据统计
			支持管理员设定统计时间维度
			统计完成的数据支持设备端展示和以报表格式导出
	报表配置	磁盘管理	支持配置报表功能的磁盘空间占比
		外部服务器	支持邮件发送服务器，以及邮件账号的设置
			支持 FTP 发送服务器的设置
			外部服务器支持联通性验证
		全局配置	支持设置报表统计的 top 用户数
			支持设置报表起始的统计日
VPN	IPsec VPN	IKE 第一阶段协商模式	支持 IKEv1
			支持主模式和野蛮模式
		加密/HASH 算法	国际标准算法(DES/3DES/AES/MD5/SHA-1)，支持国密算法
		IPsec 封装	支持 ESP 和 AH 封装
		IPsec 冷备份	支持 IPsec 冷备份，主 VPN 断开，备 VPN 触发开始建立
	IPsec 快速 VPN	IPsec 快速 VPN	支持 IPsec 快速 vpn 配置
			支持中心端和客户端方式部署
	SSL VPN	全局配置	支持配置 SSL VPN 的全局功能
		资源	支持配置 SSL VPN 发布的网路资源
		用户	支持本地管理 SSL VPN 的账号，支持对接 AD 和 Radius
		在线用户	支持对 SSL VPN 用户实时在线监控
		基础防护	支持 SSL VPN 功能网络的基础防护功能
用户管理	用户同步	snmp 同步	支持通过 SNMP 协议读取网络设备的用户相关信息，将读取的信息录入本地
		AD 用户同步	支持通过 LDAP 协议同步同步读取 AD 服务器上的用户到本地
			支持单次手动同步和多次自动同步
		ARP 扫描	支持通过 ARP 扫描的方式将扫描到的用户同步到本地
		认证后录入	支持通过各种认证策略之后将已经认证的用户同步录入到本地。作为本地用户供策略调用
	用户结构	用户组织结构	支持标准的树形结构方便管理用管理和调用用户
		临时账号	本地设置的用户账号支持设置用户有效期
	通用功能	伪 portal 抑制	支持伪 portal 抑制功能（http-APP）（命令行）

		https 弹 portal	基于 https 访问弹出认证 portal
	IPv6 支持	IPv6 用户	用户可绑定 IPv6 地址
	AAS 联动	与 AAS 通信	与 AAS 联动
	portal 逃生	portal 逃生	基于已认证用户逃生
			基于全部用户逃生
	IMC 联动	与 IMC 通信	与 IMC 联动
用户策略	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
			支持微信、短信、本地、免认证、portal 认证、AD 单点登录、二维码认证、混合认证
系统管理	系统管理员	账号管理	登录认证方式支持本地认证、Radius 服务器认证、LDAP 服务器认证
			支持系统管理员的 U-key 双因子认证
		管理设定	支持三权分立
			支持账号唯一性检查
	认证服务器	Radius	支持多用户第三方存储远端请求认证
		LDAP	支持多用户第三方存储远端请求认证
			支持 LDAP 用户、用户组同步认证
		服务器组	Radius/LDAP 服务器组，支持主备和集群
		短信认证	支持无感知认证
			支持短信验证码验证身份实现 wifi 认证上网
		AD 单点登录	支持 AD 服务器的单点登录认证方式
		微信认证	支持微信连 wifi 认证方式
			支持强制关注功能
			支持无感知认证
		混合认证	支持多种认证方式的混合认证
	系统维护设定	诊断工具	Ping、traceroute、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
		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，命令行可调比例
	双机热备 HA	主备、主主模式	支持配置、流、特征库、接口状态、IPsecVPN 状态同步
	SNMP	SNMP 配置	SNMP 代理
			版本：v1、v2、v3
		trap	trap 版本：v1、v2 Notification、v2Inform
	域名相关	DNSserver	支持 4 个 DNS 服务器
		DNS 透明代理	支持基于出接口的 dns 权重比例、优先级透明代理
	配置管理	配置管理	支持多份配置保存
			支持下次启动配置指定
			支持配置拷入，拷出备份列表
	U 盘零配置	U 盘零配置	支持 U 盘版本升级
			支持 U 盘配置导入
			支持 U 盘的零配置上线
	中英文版本	中英文版本	支持中英文版本的切换
	管理端口自定义	管理端口自定义	支持管理端口的自定义
	系统告警	系统告警	支持系统资源告警
			支持 IPsec 告警
			支持邮件和弹窗告警，弹窗告警默认展示最近 10 条告警记录
	无线非经	数据表库	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；
			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
		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；
			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