SANGFOR
深信服科技

深信服科技

SANGFOR AC 上网行为管理

产品白皮书

深信服科技股份有限公司

2015 年 09 月

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改或撤回，恕不另行通知。

深信服科技股份有限公司已尽最大努力确保本文档内容准确可靠，但不提供任何形式的担保，任何情况下，深信服科技股份有限公司均不对（包括但不限于）最终用户或任何第三方因使用本文档而造成的直接或间接的损失或损害负责。

信息反馈

如果您有任何宝贵意见，请反馈：

地址：深圳市南山区学苑大道 1001 号南山智园 A1 栋 邮编：518055

电话：0755-86627888

传真：0755-86627999

您也可以访问深信服科技网站：www.sangfor.com.cn 获得最新技术和产品信息

目录

第 1 章 上网行为管理产品应用价值

1.1 优化带宽管理，提升用户上网体验

AC 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。基于不同时间段、不同对象、不同应用的管道式流控，能有效保障用户的上网体验，保障网络的稳定性。

1.2 管控网络应用，提高员工工作效率

AC 数据中心能帮助组织管理者透彻了解员工的网络行为内容和行为分布情况。借助 AC 的管理功能，管理员能实现分时间段、基于用户、基于应用、基于行为内容的网络行为控制，据此限制员工上班时间的无关网络行为，减少员工因效率低下带来的加班、离职、薪金浪费、额外薪金支出等问题。管理员使用 AC 数据中心可自定义“员工工作效率报表”，作为员工工作效率考核的辅助依据。

1.3 管控上网权限，实现职位与权限匹配

使用 AC，管理员能依据组织架构建立用户身份认证体系，并采用分时间段、基于用户、基于应用、基于行为内容的网络行为控制，从而实现员工职位职责与上网权限的匹配，如限制研发部门不得使用 webmail 外发邮件、上班时间不能使用 IM 聊天工具，限制财务人员不能访问不受信网站，等等。以此减少越权访问和权限滥用的现象，防止泄密和不良舆论风险。

1.4 防范信息泄露，保障组织信息安全

互联网的普及让网络泄密和网络违法行为层出不穷。如果员工利用组织网络发生泄密或违法行为，而如果又没有证据，无法找到直接责任人，IT 部门将成为该事件压力的承担者。使用 AC，能帮助管理员实现基于内容的外发信息过滤，管控文件、邮件发送行为，对网络中的异常流量、用户异常行为及时发起告警，更有数据中心保留相关日志，风险智能报表发现潜在的泄密用户，实现“事前预防、事发拦截、事后追查”。

1.5 过滤不良信息，规避管理与法律风险

互联网资源极大丰富，亦良莠不齐。AC 能帮助管理员过滤违法、违规不良网页、含有不良关键字的网络信息，防止用户不慎访问不受信的网站带来法律风险。对于内网用户的外发信息行为，AC 基于内容的外发信息过滤能帮助管理员及时拦截不良言论，或者在特殊时期采用“允许看帖不允许发帖、允许收邮件不允许发邮件”的特殊管控手段，更大程度的减少舆论风险给组织形象声誉带来影响。

1.6 优化上网环境，提升上网安全

网络犯罪日益善用伪装 :利用社交网络散播 ,仿冒可信网站 ,将访问合法网站的用户“重定向”到非法网站，假冒可信软件如防病毒软件、插入非法软件，通过恶意广告、垃圾博客、恶意点对点文件传播等等。对此，对于已中毒的终端，AC 会检测网络中的异常流量如木马流量等并自动封锁并发起告警，提升局域网安全。

1.7 支撑 IT 管理，优化组织 IT 环境

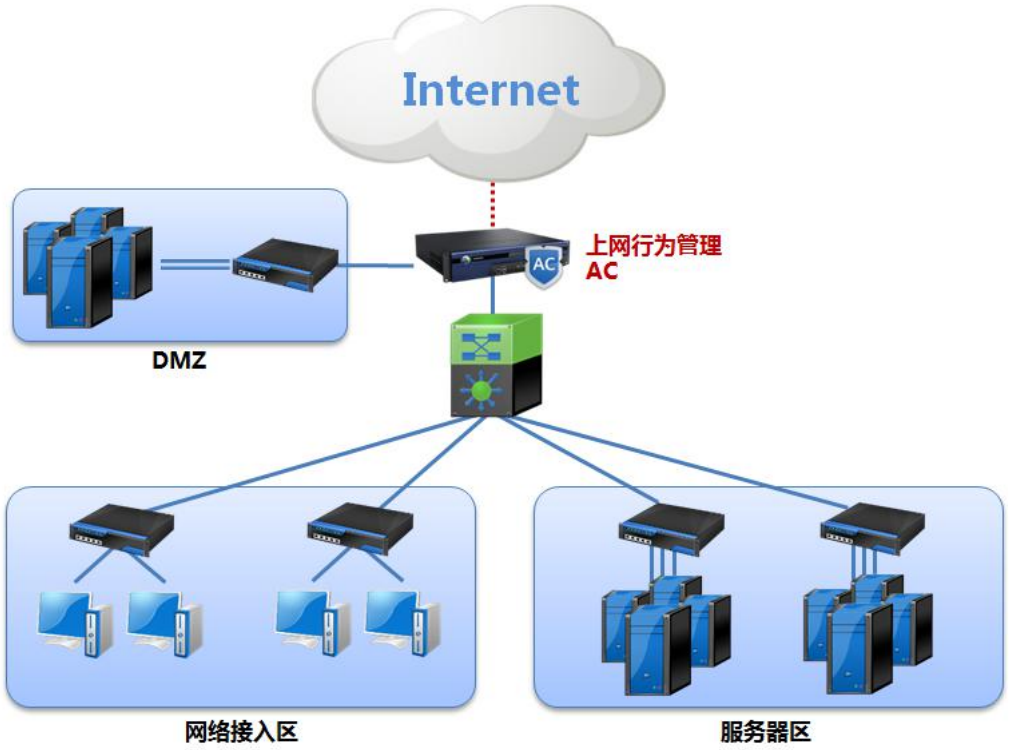
“三分制度、七分管理”，缺乏技术手段支撑的管理制度就像一道没有装锁的门，只能依赖人工值守或被管理者的自觉遵守。越来越多的 IT 管理员意识到，必须选择适合组织 IT 环境的技术手段 ,才不会让管理制度流于形式 ,AC 有效支撑组织的 IT 管理 ,帮助规范网络，减少 IT 管理员的无谓工作量，优化组织 IT 环境。

第 2 章 深信服上网行为管理产品功能

2.1 深信服上网行为管理产品部署模式

2.1.1 网关模式

网关模式是指设备工作在三层交换模式，AC 以网关模式部署在组织网络中，所有流量都通过 AC 处理，实现对内网用户上网行为的流量管理、行为控制、日志审计等功能。作为组织的出口网关 ,AC 的安全功能可保障组织网络安全 ,支持多线路技术扩展出口带宽 ,NAT 功能代理内网用户上网，实现路由功能等。



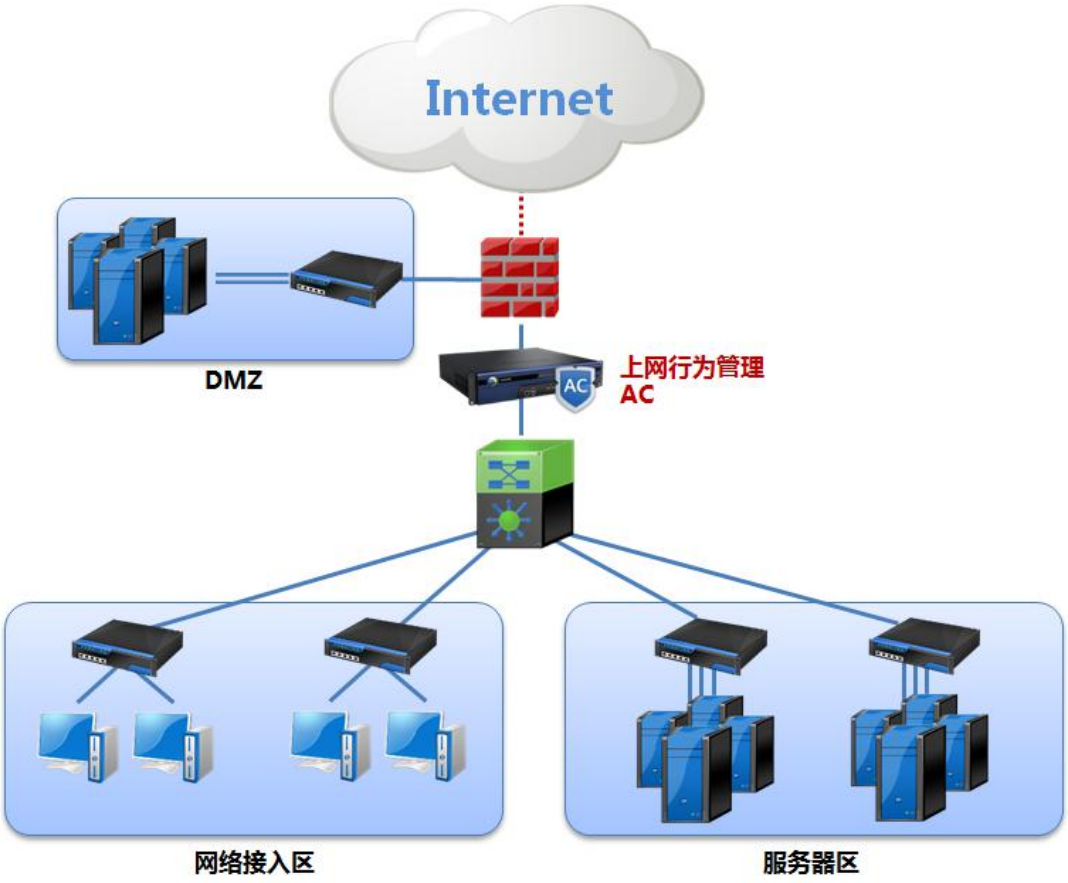
部署方式：

- AC 的 WAN 口与广域网接入线路相连，支持光纤、ADSL 线路或者是路由器；
- AC 的 LAN 口（DMZ 口）同局域网的交换机相连；
- 内网 PC 将网关指向 AC 的局域网接口，通过 AC 代理上网。

2.1.2 网桥模式

2.1.2.1 单网桥模式

网桥模式是指设备工作在二层交换模式，AC 以网桥模式部署在组织网络中，如同连接在出口网关和内网交换机之间的“智能网线”，实现对内网用户上网行为的流量管理、行为控制、日志审计、安全防护等功能。网桥模式适用于不希望更改网络结构、路由配置、IP 配置的组织。

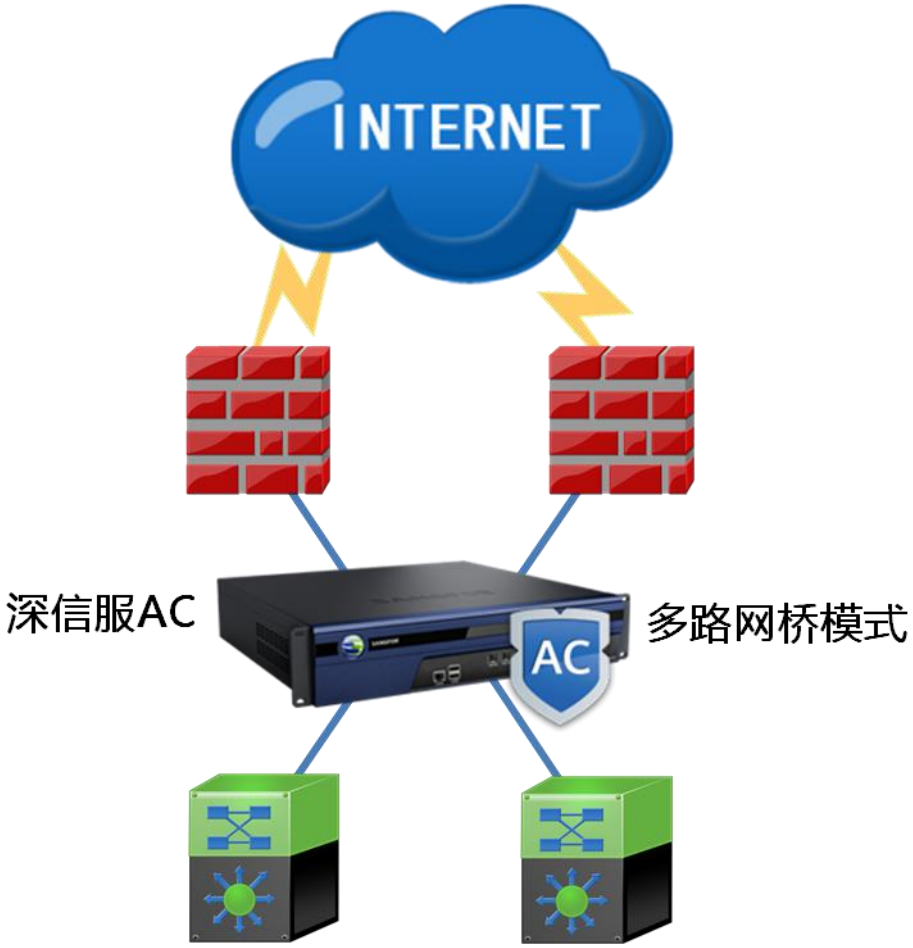


部署方式：

- AC 的 WAN 口同出口网关 LAN 口相连，为 AC 分配一个网桥 IP，该 IP 和出口网关 LAN 口在同一网段；
- LAN 口（DMZ 口）同核心交换机连接；
- 局域网内的任何网络设备和 PC 都不需要更改 IP 地址。

2.1.2.2 多网桥模式

组织考虑到网络的稳定性、可靠性，往往采用双机、双线路构建基础网络。AC 支持多路桥接模式，适应组织的多机网络环境要求。在不影响原有双机、双线路前提下，对流经 AC 的所有数据流进行审计、控制、拦截、流量管理等操作。

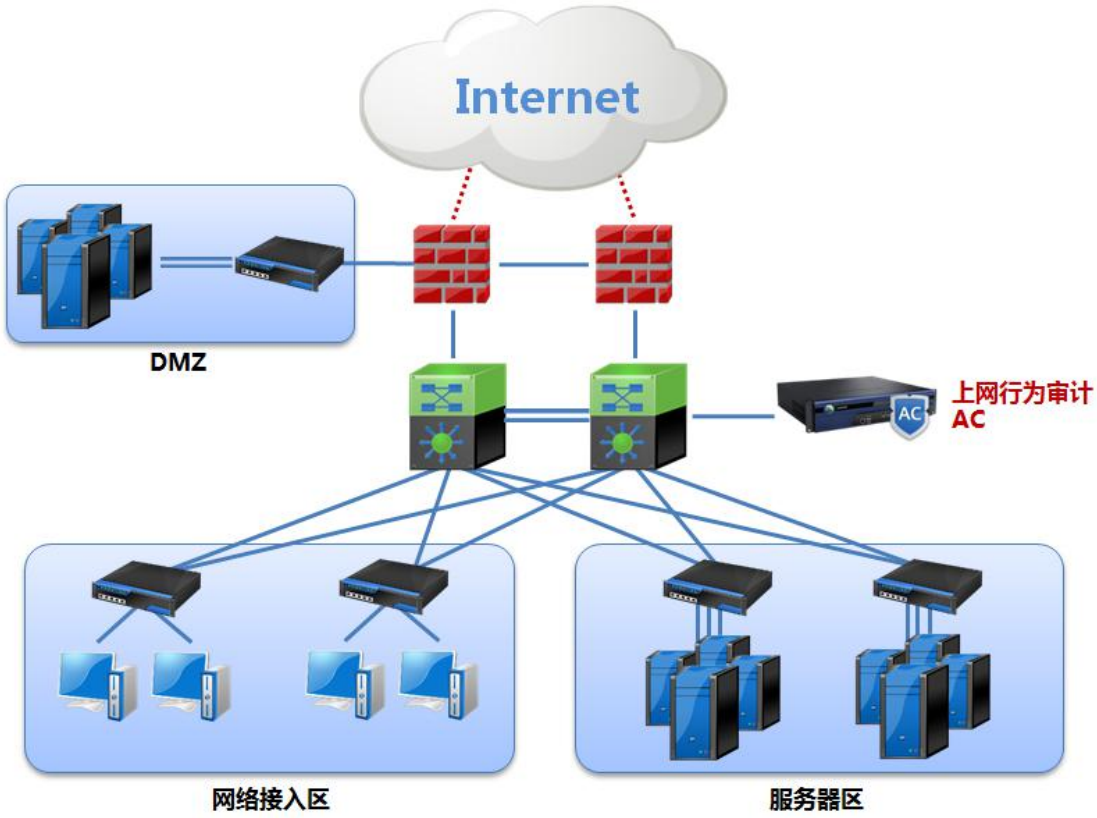


部署方式：

- 通过 AC 配置界面，定义两对桥接口（WAN1-LAN1，WAN2-LAN2）；
- 为每对网桥分配 IP 地址。

2.1.3 旁路模式

AC 以旁路模式部署在组织网络中，与交换机镜像端口相连，实施简单，完全不影响原有的网络结构，降低了网络单点故障的发生率。此时 AC 获得的是链路中数据的“拷贝”，主要用于监听、审计局域网中的数据流及用户的网络行为，以及实现对用户的 TCP 行为的管控。

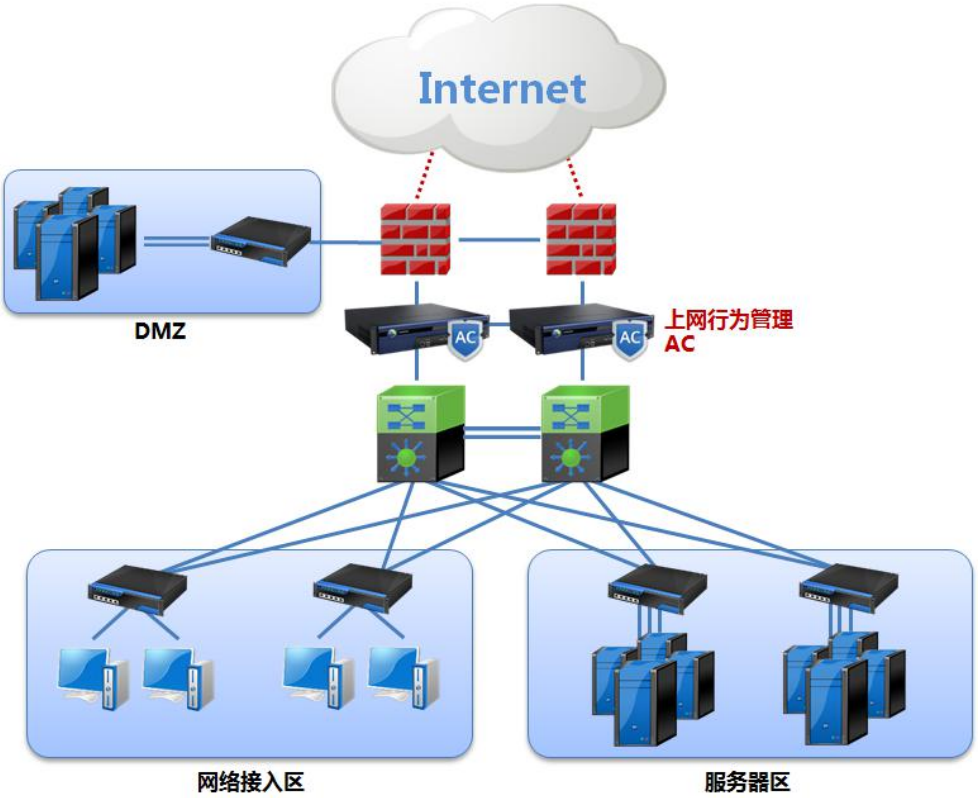


部署方式：

- 配置出口交换机的镜像端口，与 AC 的广域网口相连，实现对内网数据包的监听。

2.1.4 多机模式

组织为了网络稳定可靠，同时部署两台设备，AC 支持两台以上设备同时以主机模式运行，完美支持组织的 VRRP 环境，起到设备冗余与负载均衡的作用。在这种环境中，AC 以单网桥模式或者多网桥模式部署在组织网络中。

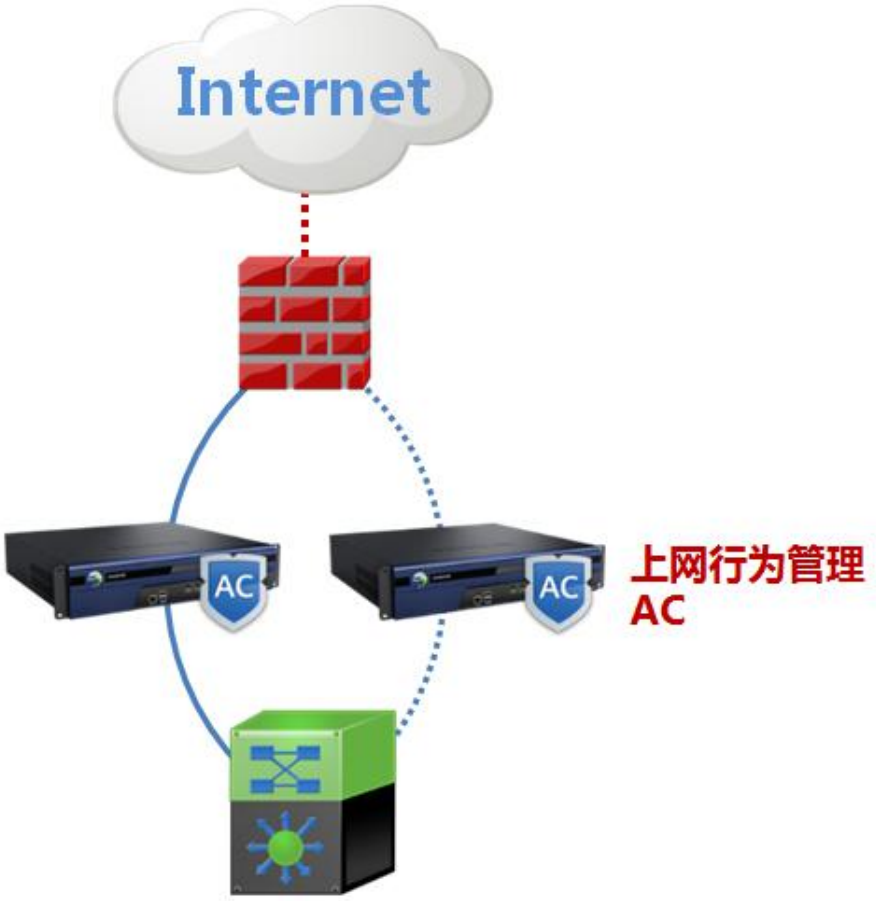


部署方式：

- AC 以网桥模式部署在网络中，为每台 AC 配置网桥 IP；
- 为每台 AC 配置同一组播 IP 地址，且每台设备上指定的通信网口在同一个局域网内，AC 之间即可实现同步。

2.1.5 双机模式

组织为了网络稳定可靠，同时部署两台设备，AC 支持两台设备以双机模式运行。两台设备通过串口线相连，一主一备，当主设备发生故障时自动切换到备用设备，提高网络的稳定可靠性。在这种环境中，AC 以单网桥模式或者多网桥模式部署在组织网络中。



2.2 身份认证

2.2.1 建立身份认证体系

有效区分用户，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。

AC 支持丰富的身份认证方式：

- 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： LDAP、RADIUS、POP3、PROXY、数据库等；
- 短信认证：通过接收短信获取验证码，快速认证；
- 微信认证：通过扫描二维码，关注微信公众号进行快速认证；
- 访客二维码认证：接待人员扫描访客手机上的二维码，备注信息后，访客即可通过认证；
- 双因素认证：USB-Key 认证；

- 单点登录：AD 域、POP3、PROXY、WEB 和第三方系统等；
- 强制认证：强制指定 IP 段的用户必须使用单点登录。

深信服 AC 短信模块不仅能够跟深信服自有品牌的短信猫对接，还能够跟各运营商的短信网关对接。部署上，为了满足有多个分支的客户需求，AC 的短信认证能够配置多个不同的 portal 页面给不同的分支使用。portal 页面还能够上传广告图片，自动滚动播放。短信认证支持二次免认证的功能，多个分支之间还能够漫游，即在 A 分支认证过，到 B 分支直接免认证。深信服 AC 的短信认证功能，既能够达到身份识别的目的，又将认证过程简化到极致，不仅神别了用户的身份，还为后续的短信营销提供精准对象，一举多得。

深信服 AC 独特的微信认证功能，为企业公众账号迅速增粉，打造一个会营销的无线网络。微信认证功能支持一键关注公众号并通过认证，适用各种终端（PC、PAD、手机）。同时，不需要在微信服务器部署代码，节省实施成本。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，用户毫无感知。不仅如此，有多分支门店的客户，门店间可以漫游认证，即在一个门店微信认证过后去其他门店可以免认证，给用户超预期的用户体验，提高企业品牌认可度。

丰富的认证方式，帮助组织管理员有效区分用户，建立组织身份认证体系，进而形成树形用户分组，映射组织行政结构，实现用户与行为的一一对应，方便管理员实施上网行为管理解决方案。

AC 支持为未认证通过的用户分配受限的互联网访问权限，将通过 Web 认证的用户重定向至显示指定网页，方便组织管理员发布通知。

2.2.2 映射组织行政结构

为了给不同用户、不同部门授予差异化的互联网访问、控制、审计权限，需要规划和建立组织的用户分组结构。

一般组织均有自己的行政结构，AC 可以完全按照组织的行政结构建立树形用户分组，实现父组、子组等多层嵌套的要求。在完成用户组的创建后，即可创建用户，并将用户分配到指定的用户组中，以实现网络访问权限的授予与继承。用户创建的过程简单方便，除手工输入帐户方式外，AC 能够根据 OU 或 Group 读取 AD 域控服务器上用户组织结构，并保持与 AD 的自动同步，方便管理员管理。

此外，AC 支持账户自动创建功能，依据管理员分配好的 IP 段与用户组的对应关系，基于新用户的源 IP 地址段自动将其添加到指定用户组、同时绑定 IP/MAC，并继承管理员指定的网络权限。管理员亦可将用户信息编辑成 Excel、TXT 文件，过 AC 的账户导入功能更加快捷的创建用户和分组信息。

用户帐号还支持有效期限定，账号过期则自动失效，支持多人共用同一帐号等，丰富的

帐号策略使得管理员可以根据实际情况自由地合理调整。

2.3 应用控制

2.3.1 应用控制策略

2.3.1.1 识别是管理的基础

网络应用极其丰富，尤其随着大量社交型网络应用的出现，用户将个人网络行为带入办公场所，由此引发各种管理和安全问题。

识别是管理的基础，全面的应用识别帮助管理员透彻了解网络应用现状和用户行为，保障管理效果。

AC 多种应用识别技术，全面识别各种应用，进而有效管控和审计。主要包括：

- 必 URL躺识别：AC躺置千万级躺RL躺库、支持基于关键字管控、网页智能分析系统躺VAS从容应对互联网上数以万亿的网页、SSL躺的容识别技术。AC躺除了内置的上百种躺RL类别以外，管理员还可以自定义躺RL躺分组，分组默认可以到躺00躺组，特殊场景可以扩容到更多组。根据组织内部特殊需求，将一些指定的躺RL躺别分到一个躺RL躺分组下，此时，各种权限策略就可以引用这个躺RL躺分组来做控制，满足精细化的躺RL控制需求，让企业内网管理更加灵活高效，更加满足“权限最小化”的管理原则。
- 醭 应用规则识别库：AC躺有国内更大的应用识别库，该库由深信服应用规则研发团队定期维护，保证库处于最新状态；该库支持躺000躺种以上网络主流应用，4500条以上规则躺能识别躺25躺种以上躺M、66躺种以上躺2P/P2P躺媒体、252躺种以上游戏、躺0躺种以上躺A、16躺种以上网银、50躺种以上金融行情软件、45躺种以上金融交易软件、13躺种木马、30躺种以上代理软件和躺90躺种以上移动躺PP，涵盖主流的网络应用；
- `& 文件类型识别：识别并过滤躺TTP、FTP、mail躺式上传下载的文件，即使删除文件扩展名、篡改扩展名、压缩、加密后再上传，AC躺样能识别和报警；
- a& 深度内容检测：IM躺天、在线炒股、网络游戏、在线流媒体、P2P躺应用、Email、常用躺CP/IP躺议等，基于数据包特征精细化识别，且支持管理员自行定义新规则，以及深信服科技及时更新和快速响应；
- 铖 智能识别：种类泛滥的躺2P躺为，静态“应用识别规则”已经捉襟见肘，通过躺2P智能识别技术，识别出不常见、未来可能出现的躺2P躺为，进而封堵、流控和审计。

通过强大的应用识别技术，无论网页访问行为、文件传输行为、邮件行为、应用行为等 AC 都能帮助组织实现对上网行为的封堵、流控、审计等管理。

2.3.1.2 上网策略对象化

AC 支持完美映射组织的行政结构，管理员可依据组织结构添加管理策略。上网策略对象化，同一条上网策略可被多个用户/用户组复用，同一用户/用户组可关联使用多条策略，实现策略和用户/用户组的双向关联，方便管理员调整。上网策略不仅仅支持生效时间调整、生效用户/用户组、应用类型限制，支持模板形式复制，更支持策略有效期，管理员可手动设定策略的过期时间，逾期自动失效，有效实现策略的回收管理。此外，AC 支持将策略的查看、编辑权限分配给指定管理员，实现策略的分级管理。

2.3.1.3 灵活的授权

AC 支持基于生效时间、用户/用户组、应用类型、位置、终端类型、SSID 的授权，帮助组织实现上网权限与工作职责的匹配，防止越权访问与泄密风险，一方面管控与业务无关的上网行为，提升员工工作效率，一方面过滤不良信息、阻止异常行为，防止法律与泄密风险。

AC 更兼顾了管理与人性化的需求，对于某些不便添加权限控制策略的部门或者是企业文化较为宽松的组织，AC 提供了“智能提醒”功能，管理员可设定允许特定用户使用指定应用的时长、流速，一旦用户使用指定应用的时长、速度超限后，AC 自动弹出提醒窗口，提醒用户注意违规行为，敦促用户自觉规范，达到促进自我管理的目的，减少管理带来的摩擦。

2.3.1.4 应用标签化

基于应用的权限划分是企业员工上网行为不可忽视的一个重要管理需求，深信服在走访大量客户的时候了解到，很多网管在针对应用配置权限的时候体验非常不好，比如：公司要求对所有具有“安全风险”的应用做封堵以保障内网安全，此时网管需要从 2000 多种应用当中挑选出具有“安全风险”属性的应用，工作繁琐单调且容易出现纰漏。

深信服 AC 给 2000 多种应用打上标签，标签根据客户需求划分为：“安全风险”、“发送电子邮件”、“高带宽消耗”、“降低工作效率”、“论坛和微博发帖”、“外发文件泄密风险”等大类。网管只用根据需求针对这六大类标签应用配置策略即可，不仅节省时间、还更加准确。

不仅如此，网管人员还可以根据实际个性化的管理需求，给应用打上“自定义标签”，以此来对这些自定义的标签应用做权限划分，满足更多个性化的需求场景，让权限划分更加灵活。

2.3.2 Web 应用控制

2.3.2.1 URL 访问控制

网页浏览是员工主要互联网行为之一，尤其随着大量社交型网站的出现，用户将个人网络行为带入办公场所，由此引发各种管理与安全问题。

在RL过滤方面，AC采用“静态RL库+云系统”的识别体系。

首先，AC内置千万级预分类RL地址库，该库由深信服RL研发小组专人负责维护，收集新增网页并经由人工审核分类，包含互联网上数十种分类站点，覆盖了95%以上用户访问量较高的网址。

其次，互联网网页容量爆炸性增长，Google声称互联网独立网址超过一万亿个，如微博等新的网址每天层出不穷，静态RL库不足以有效应对。因此，AC支持基于内容关键字的过滤手段，可基于管理员指定的多关键字过滤用户搜索行为、网页访问行为、发帖行为等。提供了人工智能的网页智能分析系统（Intelligent Webpage nalysis ystem, WAS）能够根据已知网址、正文内容、关键字、代码特征等对网进行学习和智能分类，真正帮助组织完善网页访问行为的管理。

再次，互联网上数万台AC组成了一个庞大的云网络，自动收集上报新增的、不在RL库中的网页，经深信服RL研发小组复核后，加入RL库中。

以上三重识别体系保证了AC设备的RL识别率，保障了管理员实施RL控制策略的有效性。

2.3.2.2 SSL 内容管理

SSL（Secure ocket ayer协议，被广泛地用于Web浏览器与服务器之间的身份认证和加密数据传输，利用数据加密技术，可确保数据在网络上之传输过程中不会被截取及窃听。正因为如此，一方面，越来越多的网页使用SL加密，如oogle搜索、Gmail、QQ邮箱、bbs甚至赌博网站，而因为采用了加密技术，普通的管理产品无法对其内容进行识别管理，别有用心的用户可以利用这一缺陷绕过管理，通过SL加密邮件、BBS、论坛发布的反动言论或者是向外发送组织的机密信息，导致管理漏洞；另一方面，互联网上存在大量伪造的网上银行、网上购物页面，此类网页利用了网银、网上购物等普遍采用第三方权威机构颁发的数字证书以实现SL加密的特性，伪造虚假证书以骗取用户信任，警惕性不高的用户容易在毫不知情的情况下泄露自己的账户信息，导致直接或间接的经济损失。

AC可以对SL网站提供的数字证书进行深度验证，包括该证书的根颁发机构、证书有效期、证书撤销列表、证书持有人的公钥、证书签名等，防止采用非可信颁发机构数字证书的钓鱼网站蒙骗用户，此功能亦应用于过滤SL加密的色情、反动站点，证券炒股站点等。

此外，AC 拥有专利技术“基于网关、网桥防范网络钓鱼网站的方法”（专利号 ZL200710072997.1）具有对 SSL 加密内容的完全管控能力，支持识别、管控、审计经由 SSL 加密的内容，如支持基于关键字过滤 SSL 加密的搜索行为、发帖行为、网页浏览行为，审计 SSL 加密行为如邮件发送行为，为组织打造坚固无漏洞的管理。

2.3.3 代理翻墙共享控制

许多组织统一采用 Microsoft ISA、CCproxy、Sygate 等代理服务器上网，也有的组织明文规定禁止内网用户私用代理上网，但仍有用户将浏览器等应用配置公网服务器、私装代理软件代理他人上网，甚至使用自由门、无界浏览器、IPN 等加密代理行为。由于防火墙等设备对内网用户的管理是基于目的地址和端口的，无法有效区分正常上网的流量和通过代理服务器上网的员工流量。

对于如上情况，AC 的深度内容检测技术能有效识别用户数据中包含的代理上网流量，通过代理识别模块可以识别从用户端发送到达代理服务器之间的应用数据和几个用户间的共享上网行为，进而对用户的违规行为进行管控和记录。

2.3.4 文件传输控制

利用网络来进行文件传输是许多用户每天的必修课，而在文件传输过程中存在种种管理和安全隐患，如用户通过不可信的下载源下载了带毒文件、在文件打包外发过程中不慎夹带了涉密文件、终端因为中毒或被黑客控制主动发起外发文件行为而用户对此茫然无知，有意泄密者甚至会将外发文件的后缀名修改、删除，或者加密、压缩该文件，然后通过 HTTP、FTP、Email 附件等形式外发。

AC 支持管控文件外发行为，基于关键字、文件类型控制上传/下载行为，封堵 QQ/MSN 等 IM 传文件，允许使用 webmail 收邮件而禁止发送邮件等。其中，仅仅实现对外发文件的审计和记录显然无法挽回泄密已经给组织造成的损失，单纯的基于文件扩展名过滤外发文件、外发 Email 也无法应对以上风险。鉴于此 AC 的文件类型深度识别技术能基于特征能够识别文件类型，即便存在修改、删除外发文件后缀名，或者加密、压缩文件文件外发的行为，AC 也能发现并且告警，保护组织的信息资产安全。

2.3.5 邮件收发控制

Email 不仅是组织重要的沟通方式之一，同时也是最常见的泄密方式。AC 支持基于关键字、收发地址、附件类型/个数/大小过滤外发邮件，对于将文件修改后缀名、删除后缀名，或者压缩、加密后作为 Email 附件外发，试图躲过拦截与审查的行为，AC 能够识别并进行报警。同时，对于所有收发的 webmail、Email 邮件 AC 都可以全面记录并完整还原原邮件，

并通过数据中心方便管理员对邮件日志进行查询、审计、报表统计等操作。

2.4 带宽管理

2.4.1 流量可视化

带宽有限，应用无限——组织不断地扩展互联网出口带宽，但仍然感觉不充裕，一旦内网存在网络行为不规范、滥用带宽资源的用户，IT 管理员的工作就会饱受抱怨：网络太慢、业务系统访问迟缓、页面迟迟打不开、邮件发送缓慢等。

对此，AC 为 IT 管理员提供了网络流量可视化方案，登陆 AC 控制台后，管理员可以查看出口流量曲线图、当前流量 TOP N 应用、用户流量排名、当前网络异常状况（包括 DOS 攻击、ARP 欺骗等）等信息，直观了解当前网络运行状况。

此外，数据中心（Network Database Center，NDC）对内网用户的各种网络行为流量进行记录、审计，借助图形化报表直观显示统计结果等，帮助管理员了解流量 TOP N 用户、TOP N 应用等，并自动形成报表文档，定时发送到指定邮箱，让 IT 管理员轻松掌控用户网络行为分布和带宽资源使用等情况，了解流控策略效果，为带宽管理的决策提供准确依据。

2.4.2 流量管理

当您了解了带宽的使用情况，并对带宽进行优化和分配后，我们即将对用户(组)的上网行为做进一步的管理和控制。

2.4.2.1 多线路复用和智能选路

很多组织拥有电信、网通等两条以上互联网出口链路，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？通过 AC 特有的多线路复用及带宽叠加技术，AC 复用多条链路形成一条互联网总出口，提升整体带宽水平。再结合多线路智能选路专利技术（专利号：ZL200610061591.9），AC 将出网流量自动匹配最佳出口。

2.4.2.2 基于用户/终端类型/应用/位置/网站类型/文件类型的智能流量管理

有限的带宽资源如何分配给不同部门/用户、不同应用、不同的终端和不同的业务，如何保障核心用户核心业务带宽，限制网络杀手如 BT 迅雷等等占用资源？AC 可以基于不同用户(组)、出口链路、应用类型、终端类型、位置、网站类型、文件类型、目标地址、时间段进行细致的带宽划分与分配。从而保证领导视频会议的带宽而限制员工 P2P 的带宽、保证市场部访问行业网站的带宽而限制研发部访问新闻类网站的带宽、保证设计部传输 CAD

文件的带宽而限制营销部传输MVB文件的带宽。精细智能的流量管理既防止带宽滥用，提升带宽使用效率。

2.4.2.3 多级父子通道嵌套技术

AC采用“基于队列的流控技术”，即建立管道，将不同的控制对象分配到不同的管道里。该技术的好处是控制灵活，大通道中可以多层嵌套小管道，分别基于不同的用户、时间、应用协议、网站类型、文件类型、终端类型、位置等对象建立不同的通道，同时小管道继承大通道的属性，对于结构复杂又希望实现差异化控制的组织来说可以做到为精确的控制。

2.4.2.4 动态带宽分配

组织管理员往往既希望在网络应用高峰期保障核心用户、核心业务带宽，限制无关应用占用资源，又希望在带宽空闲时实现资源的充分利用。为此，AC支持带宽的“自由竞争”与“动态分配”，除了基于父子通道进行流量控制之外，还可以根据整体带宽的利用率进行动态调整，上浮“限制通道”的最大带宽值，避免带宽浪费，实现价值。

2.4.2.5 P2P 的智能识别与灵活控制

通过封IP、端口等管控“带宽杀手” P2P应用的方式极不彻底。加密P2P、不常见P2P、新P2P工具等让众多P2P管理手段束手无策。AC采用P2P智能识别技术，不仅有效识别和管控常用P2P、加密P2P，对不常见和未来将出现的P2P功能管控。

区别于传统的基于缓存丢包的流控方式，P2P智能识别技术能够有效的从源端抑制P2P流量，释放外网链路带宽，保障核心业务的应用带宽。

对于某些企业文化较为宽松的组织，完全封堵P2P可能实施困难，AC的P2P流量控制技术能限制指定用户的P2P所占用的带宽，既允许指定用户使用P2P，又不会滥用带宽，充分满足管理的灵活性。

2.4.2.6 流控黑名单

网络管理过程中，令管理员头疼的往往不是技术问题，而是人际关系问题。很多与业务无关的应用（如迅雷下载等）不能直接封堵：封堵会造成内部矛盾；不封堵又会影响核心业务。

深信服AC根据用户需求，推出流控黑名单功能。流控黑名单是一种惩罚机制，AC可以提供基于应用的流量、流速、时长的配额限制，当用户被限额的应用超过了配额，那么该用户的这些应用将被强制加入到低速流控惩罚通道当中，限制用户的这些应用的流量到一个

较低的带宽进行惩罚。流控黑名单功能，让策略灵活，让管理更加人性化。

2.5 行为审计

2.5.1 日志记录

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展的市场规范，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，以及管理上的要求，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。AC 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。AC 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，还支持实时报警功能。

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 AC 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 AC 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 AC 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，AC 对以上行为同样可以识别并及时报警。

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。AC 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。

2.5.2 报表分析

大型组织可能在短短 60 天就产生数百 G 行为日志，仅仅实现日志的海量审计尚不足以帮助组织管理员透彻了解网络状况，而通过 AC 独立数据中心丰富报表工具，管理员可以根据组织的现实情况和关注点定制、定期导出所需报表，形成网络调整依据、组织网络资源使用情况报告、员工工作情况报告，等。报表工具主要包括：

- 首页 dashboard 功能，提供 20 张报表供客户自定义选择，通过首页 dashboard 给客户展示整体数据，帮助客户从整体上把握网络现状；

- 支持可拖拽式自定义报表，管理员可轻松配置自己关注的内容作为报表的一部分，方便灵活选择想要的数据内容；

- 智能报表模板：管理员可手动设定基于行为特征的网络概况报表、离职风险报表、工作效率报表等；

- 搜索中心：网页搜索、邮件搜索、IM 搜索、关键字搜索、论坛微博搜索等

- 趋势：流量趋势、行为趋势、IM 趋势、邮件趋势、炒股趋势等；
- 查询工具：流量查询、时间查询、用户行为查询、网站分类查询、单用户行为查询、终端接入查询、病毒日志查询、安全日志查询、操作日志查询等；

2.5.3 日志与隐私的平衡

对用户网络行为的记录一直是一个颇有争议的话题，许多组织管理员对于部署行为记录方案可能遭遇的管理阻力和舆论阻力表示担忧，主要来自“如何避免对关键人员（如组织高层领导）的过度记录”、“如何实现对日志的保护和保密”、“如何控制对日志的访问和查看权限”三方面，并希望方案提供商能给出合理的解决方法。

对此，AC 正是考虑到用户可能面临的以上风险和威胁，推出了“免审计 Key”功能。在 AC 上为总裁等高层管理人员创建帐户时使用 DKEY 认证，并勾选“不审计此用户的网络应用”选项，为总裁生成“免审计 Key”。总裁使用“免审计 Key”认证后，AC 从底层免除对总裁的所有记录。如果“非善意”人员私下取消 AC 的免审计选项，总裁再插入“免审计 Key”后系统会自动弹出警告，且禁止总裁访问网络，彻底保障信息安全。

而如何防止非授权人员访问数据中心并窥探或恶意传播他人上网行为日志，甚至导致员工对 IT 管理员的误解和埋怨？AC 的“数据中心认证 Key”技术，保证只有插入该 key 的管理员才能审计他人行为日志，否则将只能查看统计报表、趋势图线等，确保日志不被滥用。

2.6 安全防护

2.6.1 终端安全

网络世界中安全事件数量急剧攀升，内网中断、不稳定将直接影响用户的上网行为，所以需要 AC 保证网关自身安全，并强化内网可靠性、可用性。

2.6.1.1 防火墙

AC 内置基于状态检测技术的企业级防火墙，对进出组织的数据包提供过滤和控制。NAT（Network Address Translation）功能，代理内网员工上网和实现静态端口映射。同时，能够防御 DoS、ARP 等网络攻击。

2.6.1.2 网关防病毒

AC 的网关防病毒功能集成知名厂商的防病毒引擎（防病毒引擎每天自动升级），从源头对 HTTP、FTP、SMTP、POP3 等协议流量中进行病毒查杀，亦可查杀压缩包（zip，rar，gzip 等）中的病毒。

2.6.1.3 终端安全级别检测

借助网络准入规则专利技术（专利号 ZL200510037455.1），AC 将按照管理员要求检查每

位员工防病毒软件安装、运行、操作系统版本、补丁情况、注册表键值、终端程序运行情况、终端目录盘下文件情况等，不满足预设安全级别的终端将不允许访问互联网，从而提升整个内网的可靠性和可用性。

2.6.2 Web 访问质量检测

上网速度快慢是 IT 部门重点关注的内容之一，也是网络业务正常运转的直接影响因素，如何衡量用户上网体验，如何解决上网体验差，一直是令很多网管头疼的问题。

AC 的 Web 访问质量检测功能，通过检测网络中的下载速率、RTT 时延、TCP 数据重传率、连接成功率、DNS 成功率、GET 请求成功率、连接 RST 计数、PPS 突发检测等内容，以及行为管理设备的配置合理性检查，综合各项参数进行建模，提出整体网络访问质量评级，帮助网管从整体上把握网络状况。通过一些列的技术手段，AC 能够检测出网络中，AC 内外侧设备丢包和时延过大的问题、能够检测出 AC 外侧防火墙是否有连接数限制、能够检测网路中的 DOS 攻击、能够发现终端用户的 DNS 配置问题等等。通过这些问题的发现，AC 能够列出访问质量差的用户名单，并且指出故障排查方向及潜在问题原因。不仅如此，AC 还能够对访问质量差的单用户进行定向检查，并给出具体问题和解决问题建议。

通过 web 访问质量检测功能的检测、评级、排查建议等内容，能够帮助网管整体把握网络状况，快速定位网络问题并有针对性的进行排查，最终达到优化整体网络，提高用户体验的目的。

2.6.3 组织外线路检测

组织为了规范内网终端使用，避免敏感数据外泄，限制内网终端只能在内网使用，一旦接入外部网络将产生告警。深信服 AC 通过组织外线路检测技术，制定合法网关列表，一旦发现终端的网关地址不在合法网关列表内，将向管理员发出告警信息，方便管理员发现非法外联行为并迅速响应。

2.6.4 移动终端管理

随着无线移动互联网的迅速发展，智能手机、平板电脑等这些移动终端愈来愈流行，但由于 iPad 等智能终端只能采用无线网络来上网，有些员工出于便捷考虑可能自己在工位旁私自拉一些无线 AP，在公司通过无线 AP 到公司网络出口，而且这些 AP 由于安全措施薄弱，极容易被外人破解，可能导致内网暴露，信息安全遭受威胁。

深信服 AC 的“移动终端管理”功能，通过 HTTP 解析技术、系统检测技术、移动应用识别技术等多项技术，能够秒级识别移动终端，发现“非法 Wi-Fi 热点”。支持配置直接对“非法 Wi-Fi 热点”进行封堵或者发邮件给管理员进行告警等功能。提醒管理员及时做出响

应。

不仅如此，对于合法的Wi-Fi的热点支持添加到信任列表，限制封堵非法用户的同时，保证合法用户正常使用网络，业务不受影响。

2.7 无线 AP 管理

2.7.1 无线网络和接入点管理

移动互联网呈爆发式增长，其流量年增长率达到30%以上，超过整个互联网流量的的35%。这种趋势说明用户的使用习惯已经在向移动互联网倾斜。同时随着移动终端的普及和无线网络良好的用户体验，企业移动办公也迅速发展起来，因此，无线网络建设也越来越受到企业的重视。深信服的AC的开创性的提出“有线无线统一行为管理解决方案”不仅在传统的有线网络的管理中微创新，还集成无线控制器功能，直接管理的AP，一体化的管理无线网络。让有线和无线网络管理起来毫不费力。

深信服的AC能够在管理界面上直接配置接入点的工作模式，支持的Normal、Monitor的和Hybrid的三种工作模式和国家码信道；支持双频段；支持对网络协议、信道带宽、用户上限、功率、终端速率限制等各种无线射频的配置；支持信号强度和接入人数的负载均衡。

深信服的AC的支持射频智能调整，为企业提供更适合射频参数。支持泛洪攻击、欺骗攻击等入侵检测功能，同时，深信服的AC的还支持的Dos的攻击防御功能和无线网络间的用户隔离，保障企业的无线网络在开放的环境下不受安全威胁，为企业提供更加全面的安全防护。

深信服的AC的提供统一的有线无线网络的管理界面，直观实时的看到接入点状态、射频状态和无线网络状态，让网络简单易管理。

2.7.2 无线认证

网络管理的第一步是身份认证，只有识别出了用户的身份才能根据身份来做权限划分。，深信服的AC的提供三种无线安全类型：

（1）开放式

（2）WPA-PSK/WPA2-PSK（个人）和

（3）WPA/WPA2(企业)

不同的安全类型满足企业不同的安全等级下的身份认证要求。在开放式和 WPA-PSK/WPA2-PSK 类型下，支持给内部员工使用的密码认证和给访客使用的二维码认证，满足不同场景下不同角色的身份认证需求。

2.7.3 无线系统维护

深信服 AC 具备全面的无线系统维护功能，提供多种日志类型的查询，包括接入点日志、系统日志、安全日志、用户认证日志等。针对无线的 20 多个模块的日志可以区分信息、调试、告警、错误四个级别，保证日志的完整性的同时，能够快速定位到需要查询的日志。多维度、全模块的无线日志系统能够帮助管理员快速定位问题，保证出现问题之后能够有据可查，为解决问题提供全方位的线索。

深信服 AC 不仅能够提供事后被动的日志追溯，还能够为管理员提供事前主动发现问题的手段。AC 的接入点故障分析功能，管理员能够主动扫描网络内有问题的 AP，并且能够针对故障 AP 直接配置它的参数。不仅如此，对于 AP 的软件版本，深信服 AC 能够直接从管理界面做批量升级，简化管理和运维。

第 3 章 深信服上网行为管理产品技术优势

3.1 SSL 内容识别与管理

AC 拥有专利技术“基于网关、网桥防范网络钓鱼网站的方法”（专利号 ZL200710072997.1）具有对 SSL 加密内容的完全管控能力，支持识别、管控、审计经由 SSL 加密的内容，如支持基于关键字过滤 SSL 加密的搜索行为、发帖行为、网页浏览行为，审计 SSL 加密的网页内容，为组织打造坚固无漏洞的管理。

AC 不仅对加密网页能够做到内容识别与管理，对于加密的 web 邮件和客户端邮件也能做到过滤与审计。不管是 SSL 全加密的还是 TLS 半加密，AC 都能够对 smtp、pop3、iamp 等协议的邮件进行识别、过滤与审计。对于含有私有协议的特殊邮箱如：闪电邮，foxmail 和 QQ 邮箱等，AC 也做了兼容处理，能够做到和标准协议一样的效果。通过全面对加密邮件的识别过滤与审计，AC 帮助客户实现内网安全，为客户提供全方位的内容防护，防止数据泄密，填补网络管理漏洞。

3.2 P2P 智能识别技术

P2P（peer-to-peer）应用的兴起直接导致 P2P 软件及其版本的爆炸性增长，如何对 P2P 行为进行全面有效的管控成为业界的难题之一。基于 IP、端口、种子等封堵方式费时费力且达不到理想效果。AC 的深度内容检测技术对常用 P2P 软件进行识别；AC 的 P2P 智能识别技术实现对加密 P2P、不常见和未来将出现的 P2P 的彻底识别，为管理员提供了全面、高效的 P2P 行为管控手段。

能够全面识别 P2P 行为是进一步管控的基础。对 P2P 的管控包括封堵和流控两方面，既可全面禁止指定用户使用 P2P 软件，也可允许其使用但对 P2P 行为占用的带宽资源进行限制和管理，从而既优化带宽资源的使用，又为员工提供了人性化的管理方式。

3.3 免审计 Key 功能

总裁、高层领导网络访问行为，财务部收发的邮件等关乎组织机密信息，怎样避免记录此类用户的网络行为？业界多数方案是通过将敏感用户划分到指定用户组，通过设备配置界面的勾选，避免对这些用户网络行为的审计。但如果“非善意”人员私下重新配置设备对敏感用户又进行行为记录，怎么办？

AC 正是考虑到用户可能面临的以上风险和威胁，推出了“免审计 Key”功能。

在 AC 上为总裁等重要人员创建帐户时使用 DKEY 认证，并勾选“启用 DKEY 防监控”选项，为总裁生成“免审计 Key”。总裁使用“免审计 Key”认证后，AC 从底层免除对总裁的所有记录。如果“非善意”人员私下取消 AC 配置界面上“启用 DKEY 防监控”选项，总裁再插入“免审计 Key”后系统会自动弹出警告，且禁止总裁访问网络，彻底保障信息安全。

3.4 数据中心认证 key

员工、领导的上网行为日志已经通过 AC 数据中心实现海量存储，但如何鉴别访问数据中心的管理员的身份，避免行为日志被滥用(如员工的 MSN 聊天内容被传播、领导的 Email 内容被张贴到互联网上等) 而产生的个人隐私侵犯、机密日志泄漏等问题，是组织 IT 管理者和内网员工普遍关心的问题之一。

SANGFOR AC 管理员分级管理功能可实现 A 管理员登录数据中心后只能审计、查看 A 用户组的行为日志，同时配发启用数据中心认证 Key 功能后，如果没有该“数据中心认证 Key”，A 管理员登录数据中心后只能查看统计、趋势等概要信息，只有插入“数据中心认证 Key”后 A 管理员才能审计、查询 A 用户组的 MSN 聊天内容、Email 正文等详细日志信息。通过将该“数据中心认证 Key”锁入领导抽屉将实现行为日志审计查询权限的严格控制。

3.5 异常流量感知

随用户互联网访问、移动存储设备的使用、以及局域网内其他终端的感染导致用户终端设备往往存在木马、间谍软件、远程控制软件等威胁。此类恶意软件为了藏匿自己的行踪往往通过常用的 TCP 80、443、25、110 等端口与互联网控制端交互数据，这使得组织的信息安全、资产安全、网络安全等无法保障。SANGFOR AC 的异常流量感知技术正是对于以上异常流量行为进行识别并报警，帮助 IT 管理者主动发现组织内网潜藏的安全威胁，提升组织内网可靠性和可用性。

3.6 IPv6 全流量支持

随着IPv4资源耗尽，其的局限性越来越突出，在政府、教育、国外很多场景下都要求IPv6的全流量支持。深信服AC能够完整支持IPv4/IPv6混合流量、全IPv6流量的部署环境：从认证模块的本地认证或与其他认证系统单点登录，到应用识别模块的IPv6应用的识别与控制，在到流量控制模块的完整支持，最后到所有上网行为的内容审计以及日志中心的日志查询和报表，都能够毫不费力的支持IPv6环境。

第 4 章 深信服上网行为管理产品资质

4.1 市场占有率第一

来自IDC发布的2012年下半年中国安全市场研究报告表明，作为2008-2012年成长最快的安全硬件市场之一，中国安全内容管理硬件市场并未让人失望，在该市场中，更受用户欢迎的不是传统的病毒防御功能，而是Web过滤和Message安全。在安全内容管理硬件市场中，有超过17家主流安全厂商可以提供该产品，排在第一位是深信服，市场占比为41.4%，为第二位厂商的两倍以上。

4.2 深信服上网行为管理产品资质

中国信息安全产品测评认证中心《产品型号证书》

公安部信息安全产品检测中心《检验报告》

公安部信息安全产品检测中心《互联网公共上网服务场所信息安全管理系统检测报告》

公安部公共信息网络安全监察局《计算机信息系统安全专用产品销售许可证》

国家保密局涉密信息系统安全保密测评中心《涉密信息系统 产品检测证书》

国家保密局涉密信息系统安全保密测评中心《检测报告》

第 5 章 关于深信服科技

深圳市深信服科技股份有限公司成立于 2000 年，是专注于网络安全与云计算领域，致力于为用户提供更简单、更安全、更有价值的创新 IT 解决方案服务商。

目前，深信服在全球共设有 55 个直属分支机构，其中包括香港、新加坡、马来西亚、印尼、泰国、英国和美国等七个国际直属办事处和分公司，员工规模将近 3000 名。

随着企业规模的扩大发展，深信服也获得了多方认可。先后获得了“CMMI5 国际认证”、“第一批国家高新技术企业”、“国家规划布局内重点软件企业”“亚太地区德勤高科技高成长 500 强”等殊荣。同时，深信服还是 IPSec VPN 和 SSL VPN 两项国家标准的主要承建单位、并受邀参与制定《第二代防火墙标准》。在行业合作上，深信服是互联网应急中心应急服务支撑单位、国家信息安全漏洞共享平台 CNVD 成员单位、中国国家信息安全漏洞库 CNNVD 技术支撑单位和公共漏洞和暴露组织 CVE 认证合作单位。

目前，全球有近 40,000 家用户正在使用深信服的产品。其中，在中国入选世界 500 强的企业有 80%的企业都是深信服的用户。同时，凭借优秀的产品表现，深信服多款产品入围了包括国家税务总局、国家电网、建设银行、工商银行、中国移动和中国电信在内的各行业集采，各款产品均得到了广泛应用。

时刻走在行业前沿，深信服始终保持着创新能力

多年来，深信服持续将年收入的 20%投入到研发，并在深圳、北京、长沙和硅谷设立了研发中心，研发人员比例达到 40%。在对创新发展的持续投入下，深信服一直保持着每 1-2 年推出一款新产品、每季度更新 1 个新版本的研发速度。截至 2016 年 6 月，深信服共申请超过 400 项国内发明专利以及 20 项美国专利。此外，深信服是推出了全球第一台 IPSec VPN 和 SSL VPN 二合一 VPN，中国第一台上网行为管理和第一台下一代防火墙的厂商。

持续优化产品和服务，深信服快速响应市场需求

深信服研发人员每月都会进行例行的客户拜访以收集产品需求，每年都能收到超过 1000 条有效需求，并在研发工作中将其迅速转化为产品新版本。同时，深信服在深圳、长沙、吉隆坡三地设有超过 100 坐席的 CTI 中心，提供 7*24 小时的电话咨询和远程调试服务。在全国范围内，深信服在 49 个城市设立了备品备件库，配有原厂工程师第一时间提供技术支持。

进入的每一个细分市场，深信服都会努力成为 No.1

深信服的硬件 VPN、SSL VPN、上网行为管理、广域网优化等多款产品保持在市场占有率第一位；应用交付产品市场排名第二、也是排名第一的国产品牌。目前，深信服 SSL VPN、上网行为管理、下一代防火墙、广域网优化、应用交付、服务器虚拟化基础架构 6 款产品均入围了 Gartner 魔力象限，获得国际认可。

SANGFOR
深信服科技

深圳市南山区麒麟路 1 号科技创业中心 4 楼

Add: 4th Floor, Incubation Center,

No.1 Qilin Road, Nanshan District,

Shenzhen P.C.:518052

产品咨询热线：800-830-9565

Email:master@sangfor.com.cn