



SANGFOR
深信服科技

深信服科技

SANGFOR AC 上网行为管理 产品白皮书

深信服科技有限公司

2014 年 11 月

版权声明

本书版权归深圳市深信服电子科技有限公司所有,并保留对本文档及本声明的最终解释权和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容,除另有特别注明外,其著作权或其它相关权利均属于深圳市深信服电子科技有限公司。未经深圳市深信服电子科技有限公司书面同意,任何人不得以任何方式或形式对本文档内的任何部分进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。

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。

深信服电子科技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,深信服电子科技有限公司均不对(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.....	6
1.1	优化带宽管理，提升用户上网体验	6
1.2	管控网络应用，提高员工工作效率	6
1.3	管控上网权限，实现职位与权限匹配.....	6
1.4	防范信息泄露，保障组织信息安全	6
1.5	过滤不良信息，规避管理与法律风险	7
1.6	优化上网环境，提升上网安全	7
1.7	支撑 IT 管理，优化组织 IT 环境	7
第 2 章	深信服上网行为管理产品功能	7
2.1	深信服上网行为管理产品部署模式	7
2.1.1	网关模式.....	7
2.1.2	网桥模式.....	8
2.1.3	旁路模式.....	10
2.1.4	多机模式.....	11
2.1.5	双机模式.....	12
2.2	身份认证.....	13
2.2.1	建立身份认证体系	13
2.2.2	映射组织行政结构	14
2.3	应用控制.....	15
2.3.1	应用控制策略.....	15

2.3.2	Web 应用控制.....	17
2.3.3	代理翻墙共享控制	18
2.3.4	文件传输控制.....	18
2.3.5	邮件收发控制.....	18
2.4	带宽管理.....	19
2.4.1	流量可视化.....	19
2.4.2	流量管理	19
2.5	行为审计.....	21
2.5.1	日志记录.....	21
2.5.2	报表分析.....	21
2.5.3	日志与隐私的平衡	22
2.6	安全防护.....	22
2.6.1	终端安全.....	22
2.6.2	上网安全桌面.....	23
2.6.3	危险插件恶意脚本过滤.....	23
2.6.4	异常流量控制.....	24
2.6.5	组织外线路检测	24
2.6.6	移动终端管理.....	25
第 3 章	深信服上网行为管理产品技术优势	26
3.1	SSL 内容识别与管理	26
3.2	P2P 智能识别技术.....	27
3.3	免审计 Key 功能	27

3.4	外发文件深度识别	27
3.5	数据中心认证 key.....	28
3.6	异常流量感知.....	28
第 4 章	深信服上网行为管理产品资质	28
4.1	市场占有率第一	28
4.2	深信服上网行为管理产品资质	29
第 5 章	关于深信服科技	29

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，最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，AC 支持过滤危险插件和恶意脚本，防止用户终端访问被挂载的网页而染毒，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、端口扫描行为、标准端口中的非标准流量，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

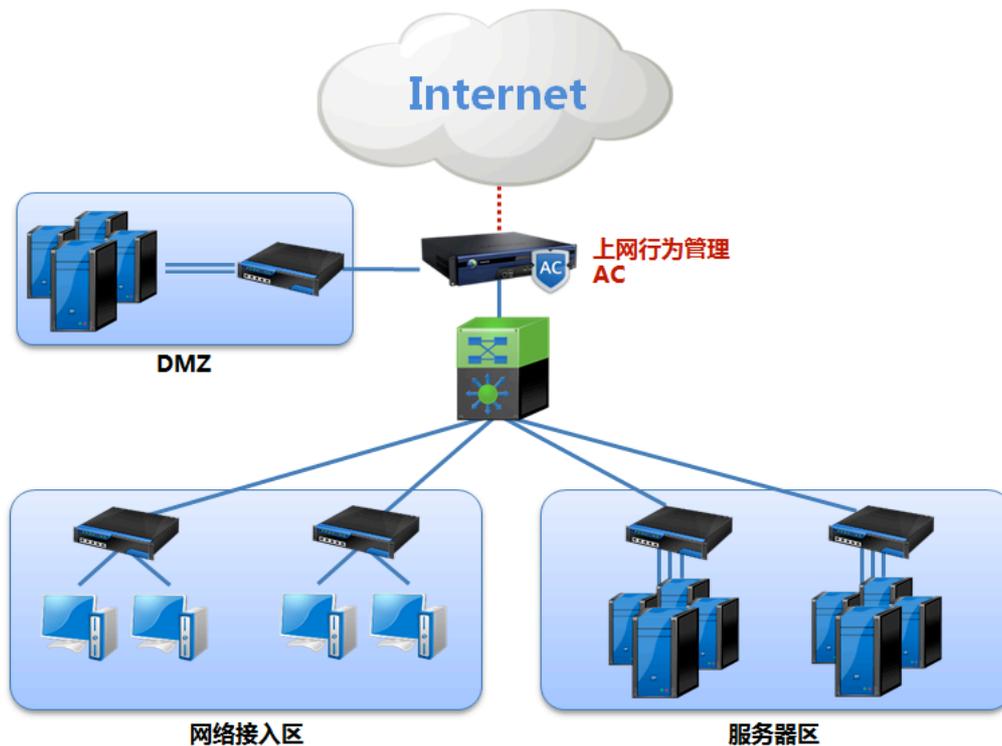
“三分制度、七分管理”，缺乏技术手段支撑的管理制度就像一道没有装锁的门，只能依赖人工值守或被管理者的自觉遵守。越来越多的 IT 管理员意识到，必须选择适合组织 IT 环境的技术手段，才不会让管理制度流于形式，AC 有效支撑组织的 IT 管理，帮助规范网络，减少 IT 管理员的无谓工作量，优化组织 IT 环境。

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。



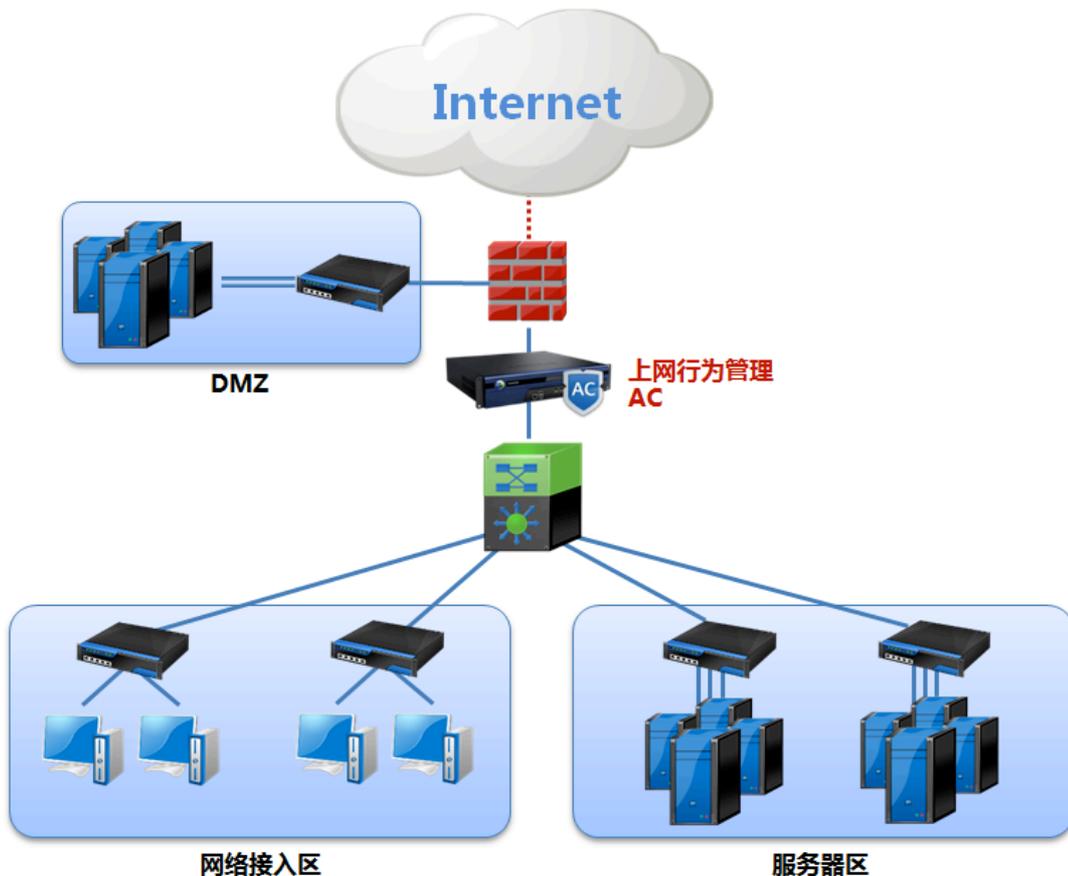
部署方式：

- 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。

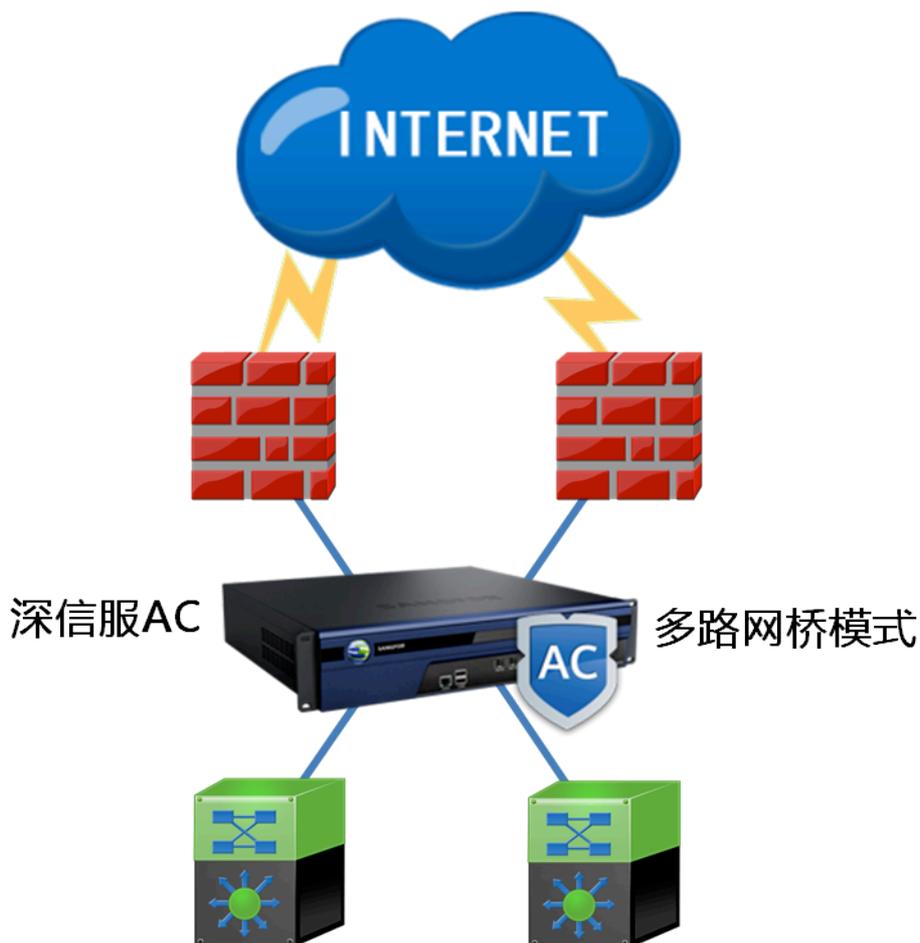


部署方式：

- 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。

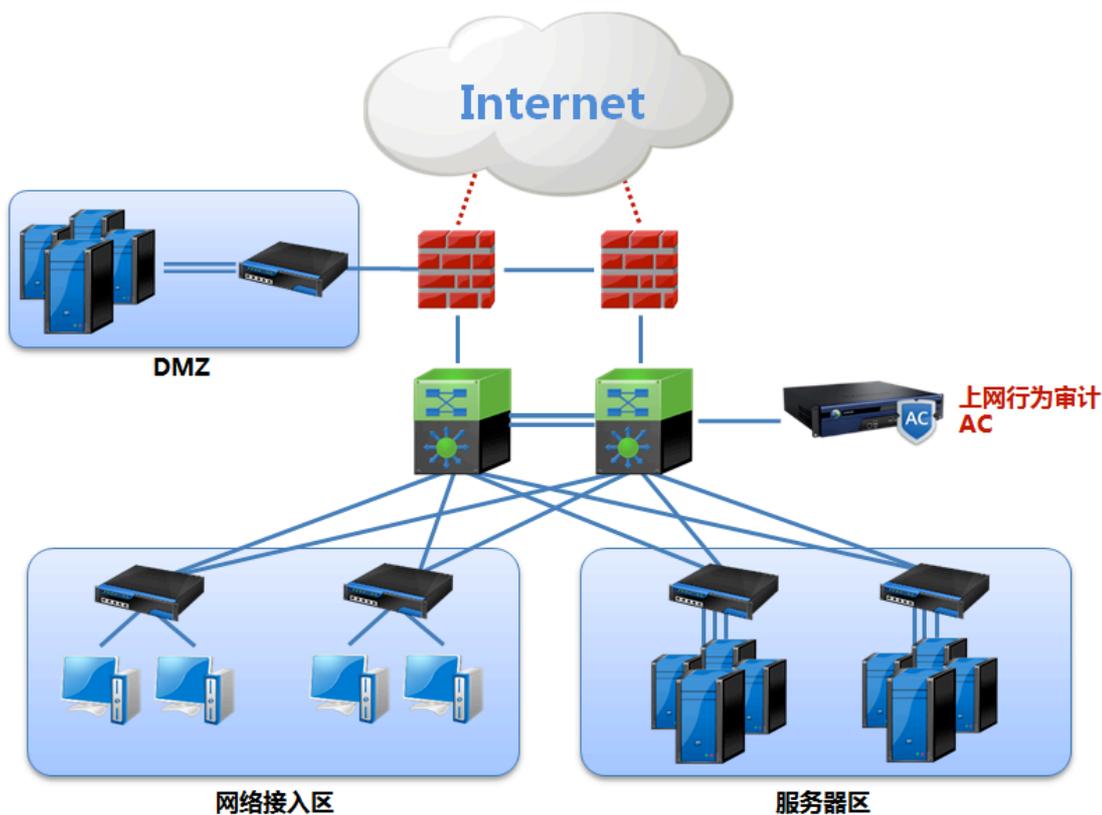


部署方式：

- 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。

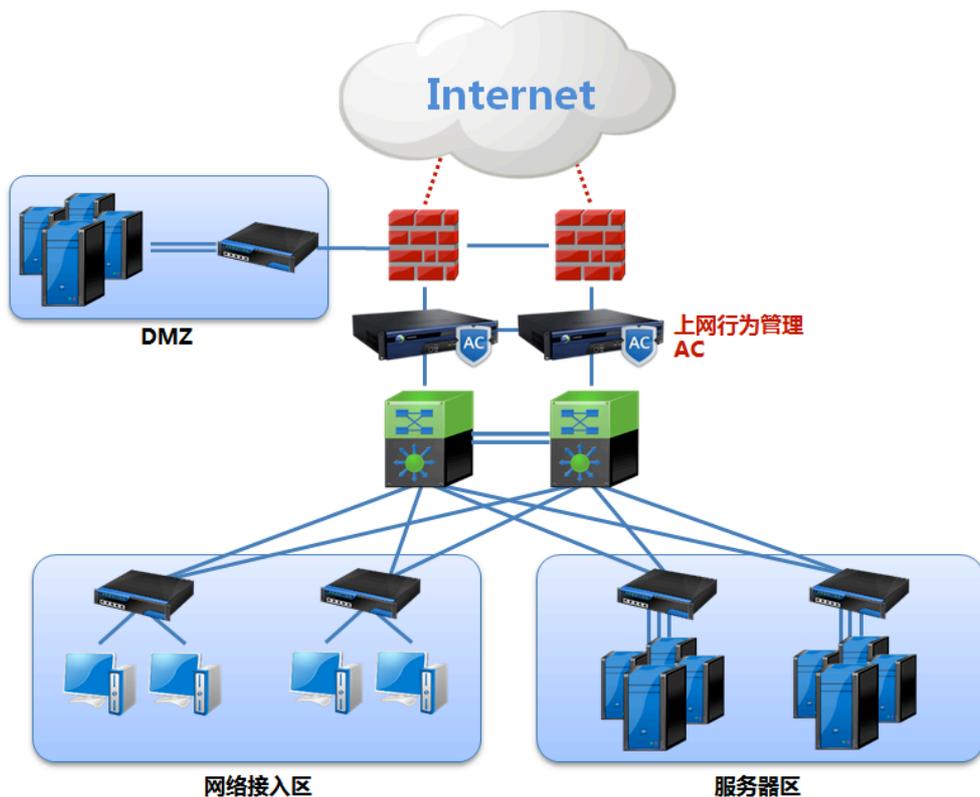


部署方式：

- 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；
- 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，不仅识别了用户的身份，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，帐号过期则自动失效，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：

- a) URL 识别：AC 内置千万级 URL 库、支持基于关键字管控、网页智能分析系统 IWAS 从容应对互联网上数以万亿的网页、SSL 内容识别技术。AC 除了内置的上百种 URL 类别以外，管理员还可以自定义 URL 分组，分组默认可以到 500 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 URL 划分到一个 URL 分组下，此时，各种权限策略就可以引用这个 URL 分组来做控制，满足精细化的 URL 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。
- b) 应用规则识别库：AC 拥有国内最大的应用识别库，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 2000 种以上网络主流应用，4500 条以上规则 能识别 125 种以上 IM、66 种以上 P2P/P2P 流媒体、252 种以上游戏、30 种以上 OA、16 种以上网银、50 种以上金融行情软件、45 种以上金融交易软件、13 种木马、30 种以上代理软件和 590 种以上移动 APP，涵盖主流的网络应用；
- c) 文件类型识别：识别并过滤 HTTP、FTP、mail 方式上传下载的文件，即使删除文件扩展名、篡改扩展名、压缩、加密后再上传，AC 同样能识别和报警；
- d) 深度内容检测：IM 聊天、在线炒股、网络游戏、在线流媒体、P2P 应用、Email、常用 TCP/IP 协议等，基于数据包特征精准识别，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；
- e) 智能识别：种类泛滥的 P2P 行为，静态“应用识别规则”已经捉襟见肘，通过 P2P 智能识别技术，识别出不常见、未来可能出现的 P2P 行为，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 URL 过滤方面，AC 采用“静态 URL 库+URL 智能识别+云系统”三重识别体系。

首先，AC 内置千万级预分类 URL 地址库，该库由深信服 URL 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%以上用户访问量最高的网址。

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 URL 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。更提供了人工智能的网页智能分析系统（Intelligent Webpage Analysis System, IWAS）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 and 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 URL 库中的网页，经深信服 URL 研发小组复核后，加入 URL 库中。

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

2.3.2.2 SSL 内容管理

SSL (Secure Socket Layer)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 SSL 加密，如 Google 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，别有用心用户可以利用这一缺陷绕过管理，通过 SSL 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 SSL 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 SSL 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 SSL 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。

一般的，传统设备处理泄密邮件时只能将其拷贝存储留作证据，但泄密邮件已经外发，损失已经造成。对此，AC 的邮件延迟审计技术（Postponed Sending after Audit, PSA），支持基于用户、邮件标题、正文、附件等特征拦截泄密邮件，并自动通知审核人员人工审核后，再将敏感邮件阻挡于内网。内网用户发送 Email 邮件时，在终端上看到已经成功发送的邮件，实际上已被全部转存至邮件缓冲区。指定的邮件审核人员会获得邮件通知，经人工审核后，才允许符合组织安全规定的 Email 邮件发送到互联网上，而不符合要求的 Email 则被截留并作为追究责任的依据，有效实现了对泄密邮件的封堵，保护了组织的敏感信息的安全性。

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 RMVB 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更为精确的控制。

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，实现价值最大化。

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 凭借 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 亦能管控。

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。

2.5 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 发布不负责任的言论、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。

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:

- 内置超过 60 多种报表模板,并支持自定义报表,管理员可手动设定时间、用户对象、应用对象、报表周期等;
- 对比报表:汇总对比、指定用户组/指定用户的对比、指定时间的对比等;
- 统计模板:上网流量/行为/时间统计、病毒信息统计、关键字报表、网络热帖报表、热门论坛报表、外发文件行为报表、危险行为报表;

- 智能报表：管理员可手动设定基于行为特征的风险智能报表，如离职风险报表、工作效率报表、泄密风险报表、异常思想倾向报表，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、行为查询、时间查询、病毒日志查询、安全日志查询、操作日志查询等；
- 内容检索：网页搜索、邮件搜索、IM 搜索、关键字搜索、Webmail/BBS 搜索等

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 上网安全桌面

深信服上网安全桌面采用沙盒技术，创造一种安全的虚拟环境，在这个环境里所做的任何对文件、注册表的修改都是虚拟的，真实的文件和注册表不会被改动，关闭安全桌面后清空一切操作。这样就可以隔离那些对整体内网安全造成危害的行为，从而让安全风险降到较低水平。同时，通过上网安全桌面能够控制默认桌面跟上网安全桌面各自的网络访问权限。

文件重定向是安全桌面对文件进行操作的一种方式，即用户在安全桌面对某个文件进行了修改，再切换到默认桌面时看到的还是该文件原先的样子。修改后的文件被放置在安全桌面的默认文件夹中加密保存，当我们切换回安全桌面后，可以直接看到修改后的文件。但如果如果没有导出文件的权限，退出安全桌面后，修改后的文件不会被真正保存。重新启动安全桌面，该文件还是保持未修改状态。注册表重定向功能与文件重定向相似，即在安全桌面内对注册表所做的更改也会备份保存，退出安全桌面后清除。

2.6.3 危险插件恶意脚本过滤

网络犯罪非法获利大，对组织网络的安全威胁也是日新月异，并且更加善用伪装：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。当用户发现时，用户端已经被安装恶意插件，被强迫浏览黑客指定的网站，或者被利用攻击某个站点，终端信息已被外发，损失已造成。

究其根源，在于用户访问不可信的资源，如现在非常流行的是通过浏览器自动安装 ActiveX 控件来进行恶意插件的传播。AC 通过对 ActiveX 控件的签名进行过滤，防止不被信任的插件安装到内网机器当中，从而解决通过 IE 浏览器乱装控件的问题，起到保护内网

安全的作用。还有形形色色的病毒、木马，而这些危害绝大部分都是危险脚本造成的。AC 通过对内网用户访问的网页脚本进行特征识别，在脚本下载到浏览器执行前进行拦截，从而起到保护内网安全的作用。

2.6.3.1 危险插件过滤

- 能识别那些下载文件是会自动安装的插件，包括所有通过浏览器自动下载的文件。
- 能根据插件白名单对插件进行过滤，内置常用安全插件列表供用户选择，还可以自定义白名单（支持插件名称、证书名称和域名）。
- 能根据插件证书的合法性进行过滤，包括：检查插件签名是否过期，对插件签名进行证书链控制。
- 能记录控件过滤日志，包括被过滤控件名称及被拒绝的原因，并能在数据中心查出来。
- 能够实现二次提示，第一次出现时做拦截，第二次实现时给出提示）。

2.6.3.2 恶意脚本过滤功能：

- 可以过滤注册表的写操作；
- 可以过滤文件的写操作；
- 过滤危险对象和危险调用；
- 能够实现二次提示，第一次出现时做拦截，第二次实现时给出提示）。

除此之外，终端用户和 IT 管理员必须在自我防护方面始终保持警惕：坚持将软件更新至最新版本、部署全面的端点安全产品、保持警觉并采用高强度密码策略、采用网络准入技术鉴定并隔离不同安全级别的终端，定期对网络流量进行审视等。

2.6.4 异常流量控制

随 U 盘等潜入组织内网的木马、间谍软件等为了隐藏自己，通常会通过常用的 TCP 80、443、25、110 等端口泄漏内网机密数据及接受黑客控制。传统设备防火墙等解决方案在开放了常用端口后并不能识别该端口中传输的数据及内容，组织的信息资产安全如何保障？黑客远程控制内网终端形成僵尸网络如何避免？AC 的异常流量感知技术能够识别常用端口中的如上异常流量，并能够实时报警，帮助 IT 管理员掌控您的网络，防范风险。

2.6.5 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。

2.6.6 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 Wi-Fi 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 80% 以上，超过整个互联网流量的 25%。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 AC 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 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 AC 能够在管理界面上直接配置接入点的工作模式，支持 Normal、Monitor 和 Hybrid 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 AC 支持射频智能调整，为企业提供最优化射频参数。支持泛洪攻击、欺骗攻击等入侵检测功能，同时，深信服 AC 还支持 Dos 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 AC 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 AC 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 外发文件深度识别

存心的泄密者往往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。仅仅实现对外发文件的审计和记录显然无法弥补由于

泄密而给组织带来的损失，单纯的基于文件扩展名过滤外发文件、过滤外发 Email 邮件也无法应对以上风险。鉴于此 SANGFOR AC 的外发文件深度识别技术基于文件特征能够识别超过一千种以上的文件类型，基于特征而非扩展名彻底遏制存心泄密者的外发泄密文件行为，保护组织的信息资产安全。

3.5 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人员的身份，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。

3.6 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。

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 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，最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

深信服科技有限公司是中国规模最大、创新能力最强的前沿网络设备供应商，致力于通过提供品质卓越的 Internet 网络设备，帮助用户业务向互联网成功转型。

深信服目前拥有 IPSec VPN、SSL VPN、上网行为管理、上网优化、应用交付、广域网加速、流量控制等多款产品，并在专业 VPN、SSL VPN、内容安全和上网行为管理等领域排名市场第 1 位。

截止 2013 年 5 月，已有超过 21,000 家用户成为深信服的合作伙伴，包括通用电气、壳牌石油、丰田汽车、中国移动等世界知名企业，以及中国人民银行、国资委、国土资源部、外交部等重要政府机构。

目前，深信服公司人数达到 1500 人，在全球设有 49 个直属代表处，包括中国内地主要城市及美国、英国、新加坡、马来西亚、泰国、香港等国家和地区。

2005 - 2012 年，深信服连续七届蝉联德勤“中国高科技高成长 50 强”及“亚太地区高科技高成长 500 强”，并被《财富》杂志评为“中国卓越雇主”。



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