SANGFOR
深信服科技

深信服全网行为管理 AC
技术白皮书

深信服科技股份有限公司

目录

1 互联网和企业内网给组织管理带来的挑战

1.1 背景介绍

随着互联网技术的发展，组织的业务模式和员工的工作模式、行为习惯都在不断发生改变：

- 网上业务：组织建设了更多的网上业务平台，通过互联网来开展业务；
- 沟通桥梁：内部员工也更加依赖互联网与外部的合作伙伴、人员进行沟通和交流，提升工作效率，获取资讯和知识，维系人脉关系；
- 移动互联网：移动互联网的消费化趋势也逐渐影响到组织内部的 IT 系统，员工更喜欢通过 WLAN、移动终端类开展工作；
- 网络接入：接入设备的种类越来越多，对于政府、企业的内部网络，工作人员办公时接入设备多种多样，包括摄像头、扫码枪、打印机等 IOT 设备；
- 业务侧访问不可视：传统互联网出口很多都部署了大量的安全设备，但是对于服务器的异常访问和下载并没有审计和分析；
- 新的法规要求：2017 年 6 月 1 日，网络安全法正式推出，其中对组织明确提出上网行为审计的要求，并且要求至少留存上网日志 6 个月。

1.2 需求分析

- **不明身份、不明终端入网造成内网安全风险剧增**

1、非法接入：外来人员拿一根网线即可接入到公司的内部网络，给公司各业务系统带来风险

2、不合规终端入网：未安装杀毒软件、不合规操作系统、终端使用弱密码等不合规终端接入网络，给内网环境带来极大的威胁，比如导致病毒内网疯狂传播

- **看似正常的上网行为，隐藏着巨大风险**

1、带宽滥用：员工上班时间使用无关应用（如 P2P、流媒体）占用大量带宽，邮件发送、资料下载、视频会议等收到严重影响，导致公司核心业务无法保障；

2、外发泄密：敏感数据/文件被随意外发，如个人隐私信息、组织机密信息、政务文件、红头文件等；无监测预警，未合规审计，不知道内鬼是谁

3、网络违法：利用组织网络进行网络造谣、人身攻击，肆意外发反动、赌博、色情信息，给公司和组织造成极大损害，且遭受法律追究；

4、上网难监管：办公室沦为免费网吧，工作效率低；先进的加密、代理技术让非法“内

容”容易绕过管控；同一个应用有好坏功能之分，管和不管两难；

- **业务访问异常行为难发现，账号滥用难管理，出现问题时难追溯**

1、业务行为不可视：员工在访问业务系统的时候，因为业务员操作进行全面审计，导致出现操作失误或数据泄密的时候无法定责

2、异常行为难发现：员工访问业务系统，可能会存在一些恶意或无意的行为对业务系统造成危害，如大量下载数据、爬取所有数据、执行删除、清空等敏感操作。

2 产品简介

2.1 硬件平台

全网行为管理 AC 系统采用软硬一体的网络设备产品形态，与具有极高的稳定性与运行效率，可方便部署于网络机房机架中。

- **高运行效率**

全网行为管理 AC 系统产品全面采用先进的 X86 64bit 架构，配合 Intel 高性能处理器与芯片组，并且在全功能开启时依然保持极高的处理能力与运行效率。

- **硬件 ByPass 功能**

硬件设计方面，全网行为管理 AC 系统具有国际先进的硬件 ByPass 功能，能够在设备宕机、关机时，使每对网络接口自动保持连同，从而使设备的网络连通性无需受到影响。此外，全网行为管理 AC 系统 ByPass 功能支持主动开启，管理员可通过设备上的硬件 ByPass 按钮或系统控制台的操作按钮进行开启或关闭。

2.2 软件系统

全网行为管理 AC 系统软件采用自主研发的高性能操作系统，并针对全网行为管理系统的各项功能进行了大量优化，从而在高负荷任务中依然保持着极强的可用性、稳定性与运行效率。

全网行为管理 AC 系统软件系统具有下列优势：

- **高可用性与稳定性**

全网行为管理 AC 系统操作系统采用自主研发的 Linux 内核，使操作系统、底层功能核心、用户界面三者具有高度的耦合性，保证了系统的高可用性与稳定性。

- **一键在线升级**

全网行为管理 AC 系统拥有完备的实时在线升级机制，用户可在授权许可期限内享受方

便的在线升级服务。只需要键入全网行为管理系统升级地址，系统会自动检测当前版本与最新版本，并可进行一键升级。

- **人性化操作**

全网行为管理 AC 系统操作模式采用 B/S 架构，用户可利用浏览器登陆全网行为管理 AC 系统管理平台。此外，全网行为管理系统在设计时就极为重视用户体验，在界面设计上采用了互联网领域先进的用户体验设计思想，例如功能模块的多标签化、审计结果的图表可视化等。

3 产品功能介绍

3.1 终端接入安全

3.1.1接入认证

3.1.1.1 网络接入认证控制技术概述

网络接入认证控制中有很多种认证方式可供企业选择，以满足企业不同需求层面、不同控制颗粒度的内网准入认证需求，主要包括以下几种：

802.1X 认证，又称为 EAPOE（Extensible Authentication Protocol Over Ethernet）认证，主要目的是为了解决局域网用户接入认证问题。

Portal 认证，指用户通过浏览器访问外网的时候，被 AC 的认证驱动重定向到 Portal 界面，只有当用户登录成功，在线信息保存在驱动中之后，数据包才会被驱动放通，实现认证控制。

MAB 哑终端免认证，支持对哑终端进行放行，比如一些打印机，扫描仪等设备，可在入网失败用户中放行，需要交换机开启 MAB 属性。

公共场所的接入认证一般使用 portal 认证，不需要安装客户端。使用 Web 页面认证，使用方便，减少客户端的维护工作量，便于运营。可以在 Portal 页面上开展业务拓展，如广告展示、责任公告、企业宣传等。

对于严格管控内网接入的场景，使用 802.1x 认证，在没有认证之前不能访问内网（包括二层网络也不能接入），即不能经过二层交换机，满足企业对内网的严格准入控制。

对于哑终端或是自助终端可以使用 MAB 认证，对于企业希望免认证直接上线的设备也可以采用这种认证方式，实现全网终端方便快捷上线，简单安全入网。

三种认证方式的对比如下表：

控制点	认证方式	适用场景	适用对象
二层接入控制	802.1x 认证	1、 需要交换机配合，且需要安装客户端（实施较复杂） 2、 未认证前同一个交换机下的 PC 之间也不能互访，管控严格。	员工
	MAB 认证	1、 需要交换机配合，不需要安装客户端（实施复杂度中等） 2、 未认证前同一个交换机下的 PC 之间也不能互访，管控严格。	哑终端 自助终端 免认证设备
三层接入控制	Portal 认证	1、 交换机镜像数据即可，一般只有核心对三层交换机支持，不需要安装客户端（实施简单） 2、 可支持多种认证方式，密码认证、AD 域认证、短信认证、微信认证、单点登录认证等均可支持 3、 控制点在三层核心交换机上，未认证前，不能上互联网网、不能访问业务系统；但核心下面的二层交换机 PC 之间可以互访。	员工 访客 哑终端（绑定 MAC，做免认证）

3.1.1.2 深信服终端接入认证技术概述

有效区分用户，是实现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。深信服 AC 支持丰富的身份认证方式：

■本地认证：用户名/密码认证、IP/MAC/IP-MAC 绑定，支持绑定短信和微信快捷认证；

■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；

■OA 认证：支持通过 OAuth 认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证；

■会议室二维码认证：支持提供二维码和会议号，用户扫码或输入会议号认证上网；支持通过验证手机号码实名认证；

■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、用户密码+动态令牌认证；

■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。

■802.1x 认证：交换机端口授权的认证方式，能够在认证通过之前有效阻止 PC 的 TCP 和 UDP 报文，实现二层的强管控。

■MAB 认证：基于 802.1x，支持哑终端通过 MAC 认证的方式接入网络，

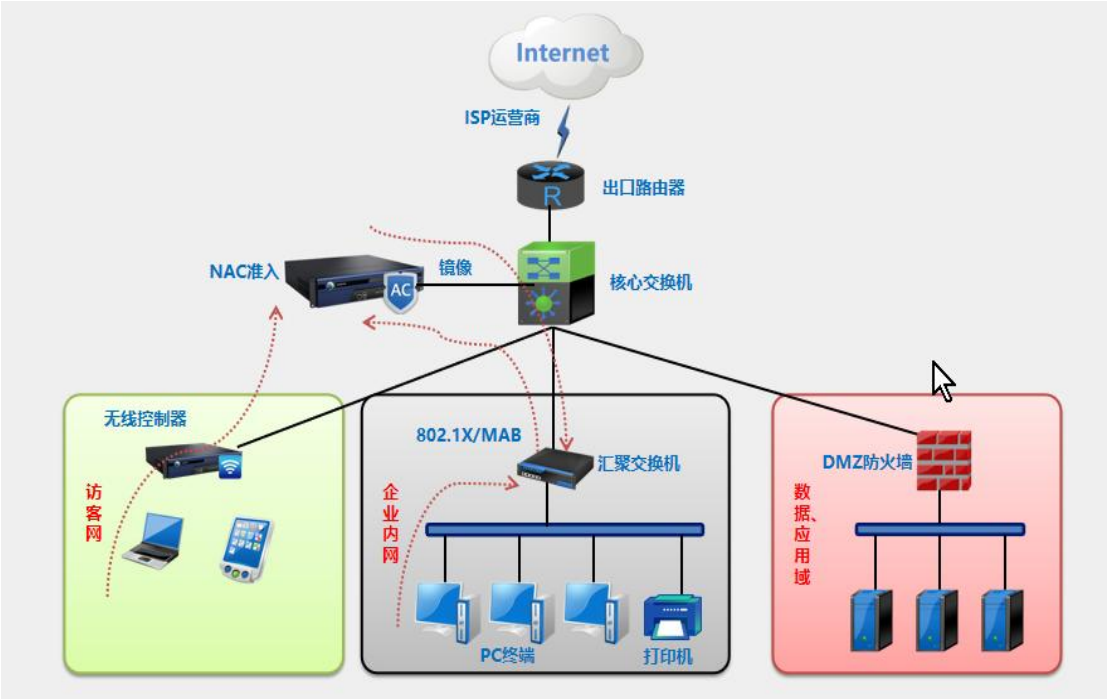
■CA 认证：支持基于 802.1x 的外部 CA 证书认证，同时支持在线证书状态查询（OCSP）；

3.1.1.3 802.1x 技术方案介绍

802.1X 认证，又称为 EAPOE（Extensible Authentication Protocol Over Ethernet）认证，IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1X 协议。后来，802.1X 协议作为局域网接口的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题,或解决局域网用户接入认证问题。

802.1X 系统为典型的 C/S 结构，包括三个实体：客户端、接入设备和认证服务器，有以下几个特点：

- 安全性高，认证控制点可部署在网络接入层或汇聚
- 需要使用 802.1x 认证客户端（AC 准入 agent）或操作系统自带的 802.1X 客户端。使用 AnyOffice 时可以根据终端检查结果规格隔离于和后域。
- 技术成熟，被广泛应用于各类型园区网员工接入



AC 支持使用客户端（agent）来实现 802.1x 认证，这种认证方式需要在二层交换机/无线控制器上启用 802.1x，实现有线或无线环境下的二层准入控制，具有很高的安全性。用户接入二层网络就需要进行认证，认证通过之后才能获取到 IP 地址访问内网资源，没有认证前不能访问内网，即不能经过二层交换机。结合交换机做 802.1x 认证的实现原理：

- 在汇聚交换机或无线控制器上启用 802.1x
- 在终端上安装 AC 准入认证客户端（agent）
- 未认证的终端用户禁止访问内网或是仅能访问 guest vlan 访问有限资源

◆ 终端用户经过认证后才可以入网

3.1.1.4 Portal 技术方案介绍

Portal 认证不需要客户端，实现原理是用户优先获取 IP 地址，访问某 url 被重定向到 portal 认证页面，输入用户名密码进行认证，完成认证即可访问相应资源，实施简单便捷，对原有网络环境没有影响，安全性适中，认证通过前可以经过二层交换机。通过这种认证方式，可以实现不需要认证（绑定 IP/MAC）、账号密码认证、单点登录、禁止上网、微信快捷登录以及短信快捷登录。

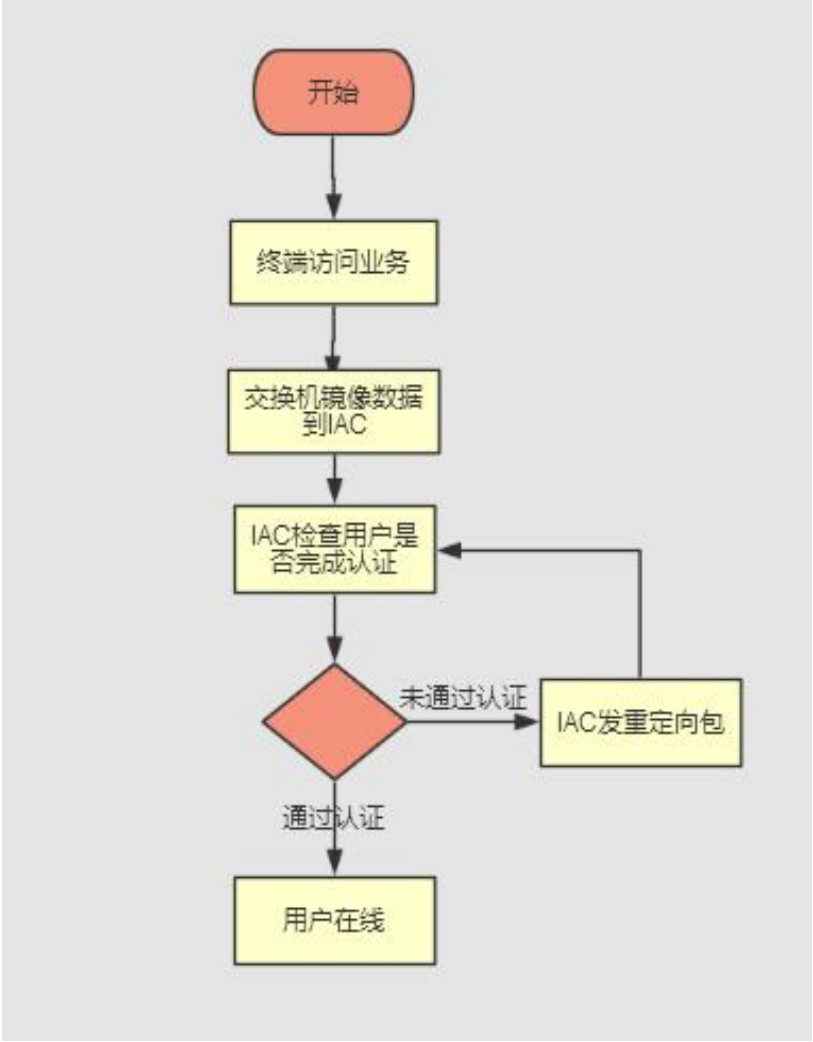
认证流程：

1.终端访问业务或上网数据经过交换机，交换机镜像数据包到 AC 上，AC 检查终端是否已经认证过了，如果没有认证，则发 302 重定向包；

2.终端接到 302 重定向包，到 AC 设备上进行认证；

3.认证通过后不再发重定向包，进行放行；认证不通过的，发 reset 阻断用户对业务的访问；

4.如果客户除了认证，还需要检查终端合规以后才能正常接入网络，则需要添加终端检查策略，在用户认证完成同时检查终端合规以后才能访问内网资源。

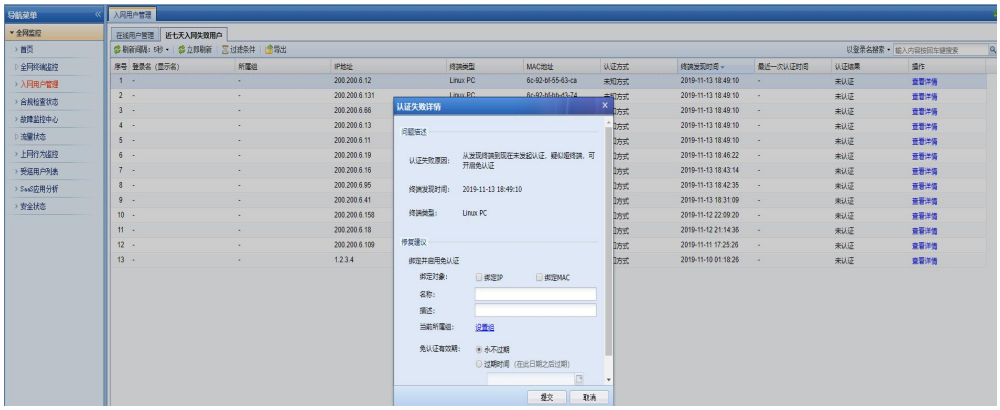


Portal 认证优点：支持旁路部署，易实施，低干扰；可以实现业务接入控制，认证通过前不能通过核心交换机访问业务系统；全网流量可视，支持互联网审计和业务审计，同时满足接入控制需求。

3.1.1.5 MAB 技术方案介绍

MAB 全称为 Mac Address Bypass，当启用 IEEE 802.1x 认证的端口连接的设备是打印机（或者其他无法进行交互认证的设备）时，应当使用此特性。如果交换机等待客户端返回 IEEE 802.1x 认证的 EAPOL 响应包超时，交换机就会尝试使用基于 Mac 地址的免认证特性来识别客户端。同时使用 Mac 地址作为客户端的身份标记，把客户端的 Mac 地址作为用户名和密码发送给认证服务器。

MAB 认证优点：无需装端，适用于物联网场景，支持哑终端设备、自助设备、服务器等不适于做认证交互的终端设备；可以实现二层接入控制，认证通过前不能访问内网；支持对哑终端进行放行，比如一些打印机，扫描仪等设备，可在入网失败用户中放行,进而对哑终端的 MAC 绑定，通过 MAB 实现认证。



3.1.2终端资产发现

公司的 IT 管理员，往往希望能够总览公司内网全局网络分布使用情况，查看终端设备的部署使用情况，IP 分配情况，甚至内网中网络设备（交换机、路由器、防火墙等）的分布使用情况，AC 做到了让管理员能时刻掌握网络资源分配和使用，为优化网络提供全面、第一手的数据。

3.1.2.1 终端发现

AC 支持扫描到内网中的指定网段中网络终端设备，并对扫描到的设备进行设备类型识别。可以分析出镜像流量到 AC 的终端设备的终端指纹信息（设备类型、IP、MAC、操作系统、在线状态、开放的端口、厂家等基本详情），AC 支持通过 tcp、dhcp、arp、http（https）、dicom 等协议识别终端特征，真实环境测试下发现率和识别率远高于国内厂家设备，支持 PC、移动设备、哑终端、专用设备的发现和型号识别：支持 Windows、Linux、MAC、瘦客户机等 PC；支持手机、平板等移动设备；少支持服务器、交换机、无线控制器等 7 类以上网络设备；至少支持打印机、投影仪、电视、摄像头、门禁系统等 10 类以上哑终端；

考虑到设备扫描时间真空，通过定期扫描（比如每天全网扫描一次、每两小时重新扫描到的但没有解析的设备）使扫描过后才接入网络的设备无法隐藏。

同时支持新设备发现趋势、终端违规检查项排行、终端违规用户排行，帮助管理员直观掌握终端接入安全状态；

为什么 AC 能做到提供如此重要的网络使用终端信息数据，让管理员如同得到上帝视角一般穷览内网全景，目前采用了主动识别和被动识别机制。

主动识别

主动识别采用了开源嗅探工具来主动探测指定网段内的设备信息，根据不同设备的 TCP/IP 协议栈的差异，与已知的内置设备指纹库匹配得出具体的操作系统信息，通过本机的 ARP 信息获取设备的 mac，再根据 IEEE 标准规范，用 MAC 匹配对应的厂商。通过内置脚本，完成探测并识别其他哑终端设备类型。

被动识别

被动式就是不主动发送数据包，通过抓取流量信息，进行分析获取相应的设备信息，被动识别主要采用的技术手段：

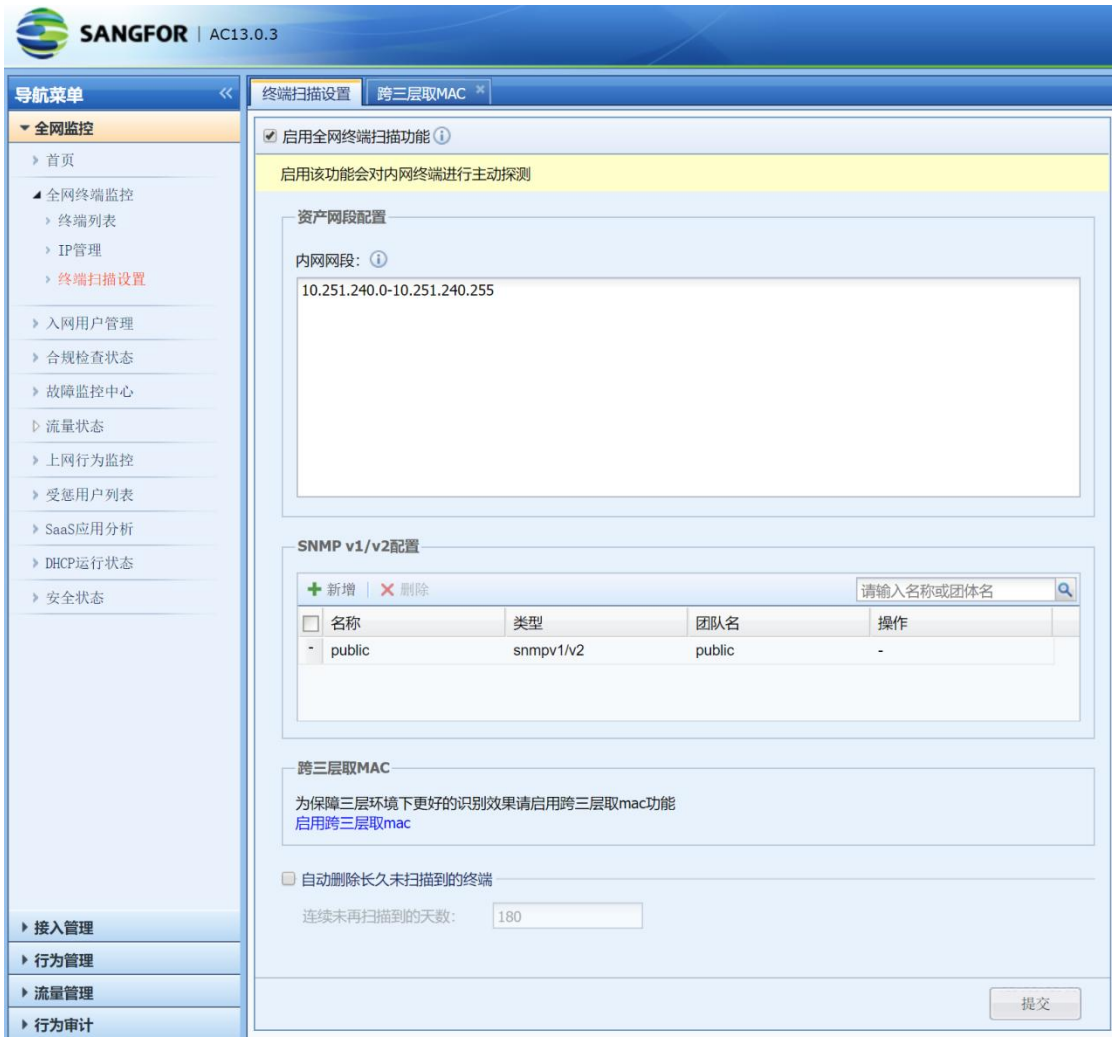
http： 通过 http 流量的字段信息，能够获取设备的终端型号等信息

Dhcp：分析 dhcp 的 request 包，分析其中指定字段信息，提取厂商、主机名特征标识，将这些信息作为终端类型识别的指纹，与一个事先维护的已知终端厂商标识库匹配，确定终端厂商、主机名信息。

设备部署

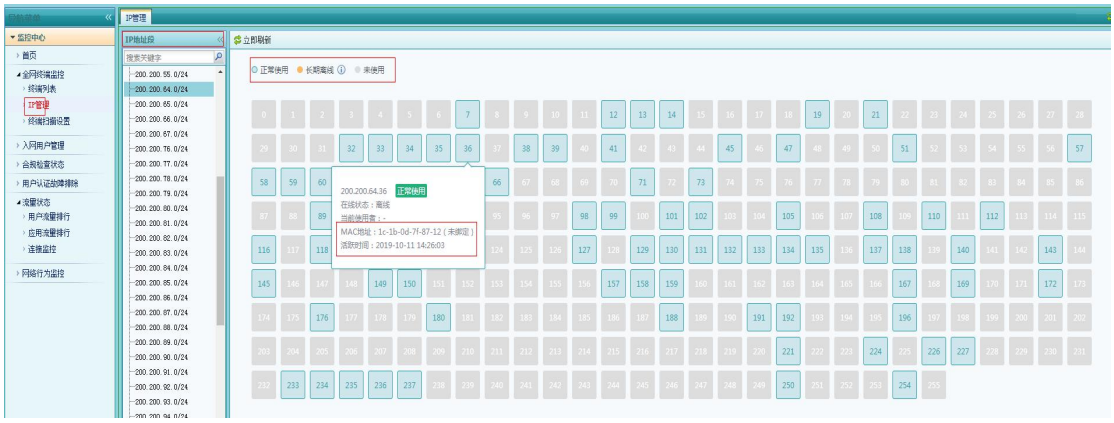
二层部署 nmap 能通过 arp 来得到 mac 信息，三层部署利用跨三层 mac 数据和 snmp 取交

换机 arp 信息来得到 mac 信息， 其余嗅探方式（smb、onvif、snmp）均支持三层场景。



3.1.2.2 IP 梳理

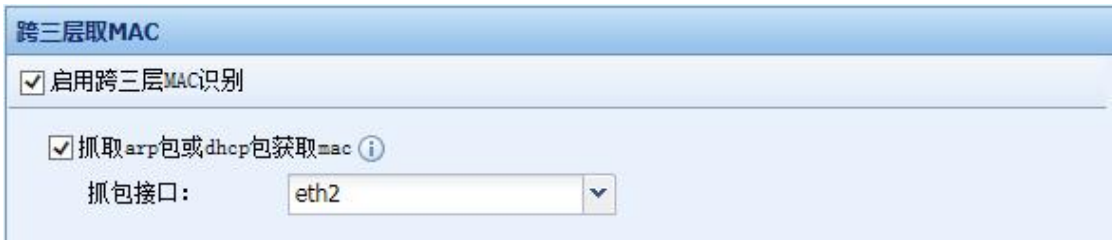
AC 支持主动扫描到内网中指定网段的 IP，也能通过解析出镜像到流量的设备的 IP，这里可以让管理员尽览内网 IP 使用情况，为 IP 分配和管理提供第一手资料（正常使用 IP、长期离线 IP 和未使用 IP，以及正常使用 IP 的在线状态、使用者、MAC 地址和活跃时间）。



3.1.2.3 跨三层取 mac

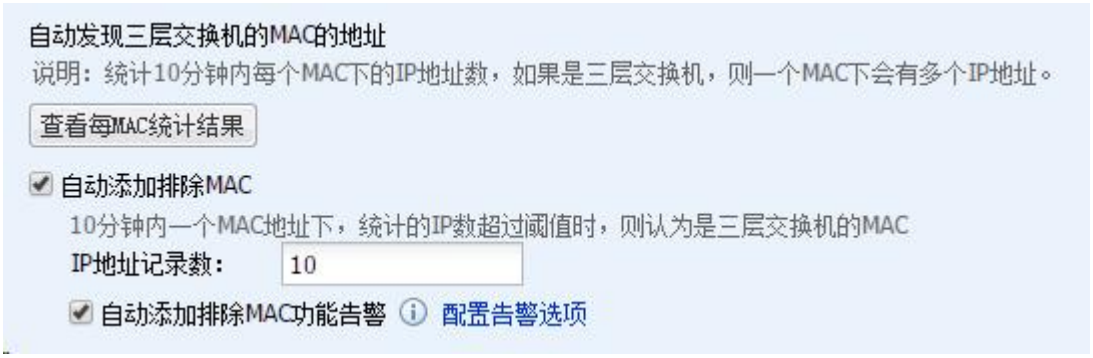
AC 支持两种不同方式的跨三层取 MAC。当内网用户绑定 MAC 地址或者限定了用户的 MAC 地址范围，并且内网是跨三层的环境下，如果想实现 MAC 免认证，需要开启跨三层取 MAC，来解决三层网络环境取不到 MAC 的问题。

第一种是通过镜像读取内网用户的 MAC，不需要交换机启用 snmp 协议，将 AC 任意一个空闲的网口接到交换机，交换机对应的接口启用镜像，将相关数据包镜像到 AC，通过抓取 ARP 包或者 DHCP 包获取 MAC。



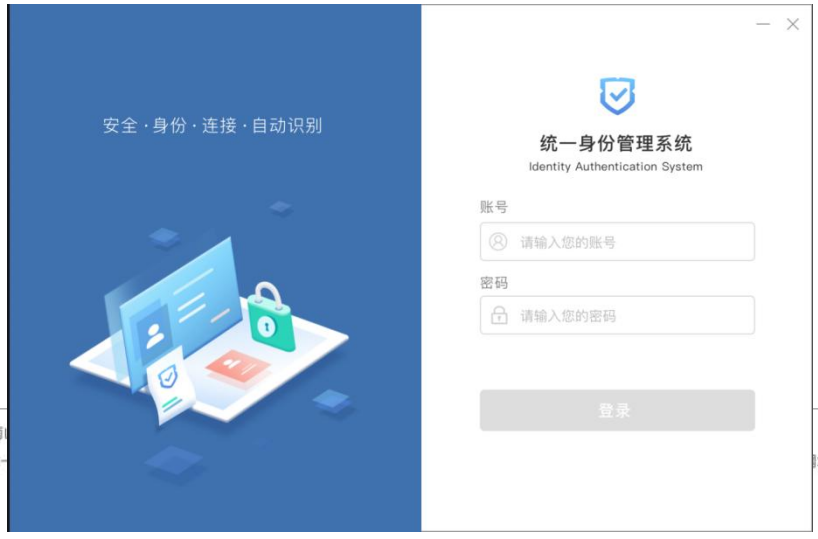
第二种是利用内网交换机的 SNMP 功能，通过 SNMP 协议获取交换机上内网用户真实的 MAC 地址。设备上会定期发 snmp request 到三层交换机请求交换机的 MAC 表，并保存在设备内存中。此时如果三层交换机其它网段的电脑经过设备上网时，如一台 PC 192.168.1.2

（和设备 lan 口不在同一网段）经过设备上网，该 PC 数据包经过设备时，设备校验此数据包的 MAC 是三层交换机的 MAC，则对此 MAC 不做处理，而根据 192.168.1.2 这个 IP 去内存中查找其真实的 MAC 地址，实现对用户真实 MAC 的验证。

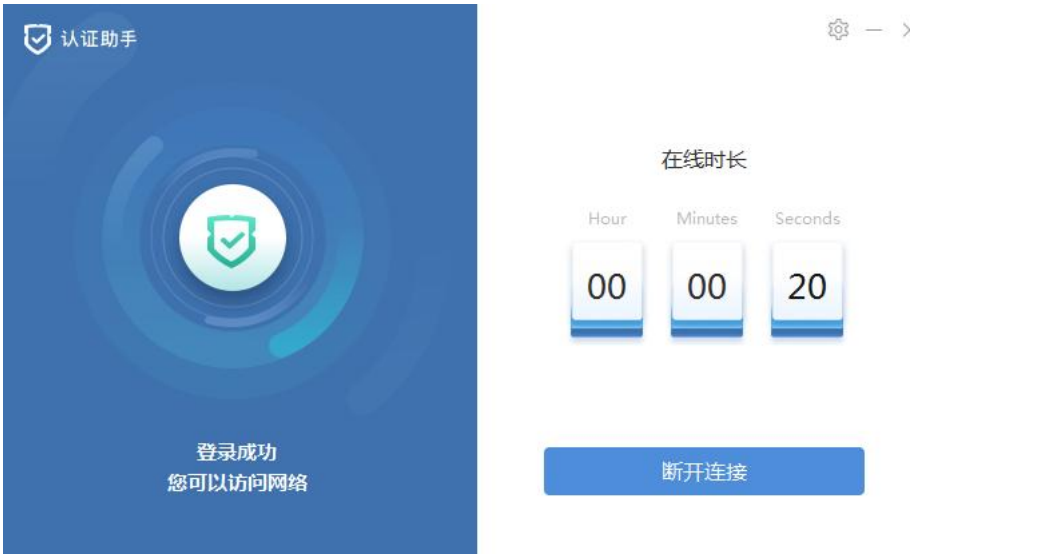


3.1.3终端轻量级安全插件

为了优化企业的入网体验，深信服全网行为管理 AC 推出了轻量级插件解决方案，一个简单易用的小插件集准入认证客户端、终端安全性检查、终端安全管控、客户端应用审计、SSL 插件解密于一体，满足客户对终端安全的需求。



当前轻量级客户端仅支持 PC 的 WINDOWS 操作系统。轻量级插件安装包在 10M 左右，内存占用 8M 以内，CPU2%以内，可以对终端用户做到无感知。轻量级插件具有一定的安全性，员工不能随意卸载。



3.1.3.1 插件安装推送

推送安全插件有几种方案：重定向页面统一推端、使用域推、使用桌管推送；AC 支持两种不同的轻量级插件安装包：传统安装包和静默安装包；其中，重定向页面可以选择终端员工自行安装的安装包文件，域推送或桌管推送可以选择无感知静默安装文件。

3.1.3.2 终端 All in one（AIO）

AC 终端安全插件支持与深信服 aTrust 客户端、EDR 客户端集成，实现客户端统一安装、

统一托盘、统一客户端工作台（统一入口）、联动推端状态可视，桌面快捷方式统一等功能。【目前支持 Windows 客户端】

3.1.4终端安全检查和修复

3.1.4.1 安全检查

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进行合规性检查，包括杀毒软件检查、登录域检查、操作系统版本、进程、文件、注册表、计划任务、补丁情况、外联检查、Windows 账号、防篡改、客户端集成、软件安装检查等安全合规项，不满足预设安全级别的终端将不允许访问互联网或是限制其访问权限，从而提升整个内网的可靠性和可用性。

3.1.4.2 修复和处置

全网行为管理 AC 平台对入网终端进行合规性检查支持隔离修复功能，内置的终端合规性检查策略包括：常规检测：支持 windows 补丁检测，可按照指定级别或指定补丁进行检测，提醒用户及时修复；检测注册表不安全项，支持自动删除该项，或是禁止上网并提醒用户修复；及时发现可疑文件检测，支持自动删除文件，对用户进行禁止上网及告警，同时上报给管理员；检测是否运行指定进程，支持自动停止进程，对用户进行禁止上网及告警；对操作系统检查，支持对用户进行禁止上网及告警；对指定软件是否安装检查，对不满足检查要求的终端可安装指定软件、弹窗提示、只记录结果、禁止上网；支持自定义计划任务，制定时间执行客户定义程序并检查执行结果；支持登录域检测（PC 以任意域账号登录即可检测合规）和登录指定域（PC 以域账号登录到指定域中的一个即可检测到合规）。对于违规终端，支持禁止上网，提示用户，只记录结果和限制用户权限四种违规处理方式。

3.1.4.3 杀毒软件检查和修复

基于 AC 轻量级插件方案和无端方案，对于杀软检测支持插件杀软检查准入规则以及流量杀软检查准入规则，保障入网终端安全性。

插件准入规则支持检测主流杀软有无运行，同时支持杀软版本号检测；对于违规终端，支持禁止上网，提示用户，只记录结果和限制用户权限以及违规修复五种违规处理方式，其中限制用户上网支持选择访问权限策略和用户限额策略两种违规处理，违规修复支持运行指定程序修复和重定向指定页面修复两种不同的方式。

支持 20 款以上主流杀毒软件的运行情况、软件版本、病毒库更新时间检查,更多杀毒软件的检查策略可通过“进程检查”自定义添加。

AC 创新支持无需安装客户端，通过流量状况检查 10 款以上主流杀毒软件的运行情况，为客户交付轻量级的软件检查方案，该功能主要基于识别杀毒软件的客户端与服务器间心跳通信的流量包实现，违规操作支持定时重定向到指定网址和只记录结果。

3.2 终端轻量级桌面管控

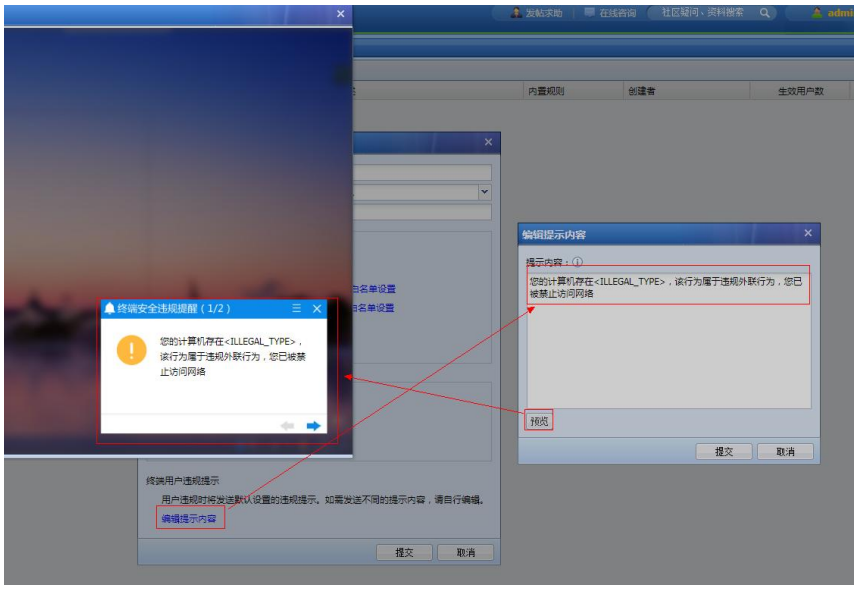
深信服关注到用户办公网在新形势下所面临的安全威胁挑战逐渐升级，上网行为管理 AC 在原有管控互联网的基础上，基于多年的技术积累将能力延伸到管控全网的用户、终端、

应用和数据，升级为全网行为管理 AC，提供网端一体化安全管控能力，管好人的同时更好管好终端，构建有效的办公网安全管控体系。

3.2.1非法外联

安全入网后需要解决的另一个问题就是如何防止非法外联，AC 支持从外联检查和外联控制两个不同的层次加强对非法外联的管控，全面保障内网安全。

外联检查顾名思义是用于检测上网终端设备上外设的使用情况，AC 通过外联类型配置、违规处理、提示用户 三方面来完成外设管理，在检查项配置中，AC 提供了拨号行为、双网卡行为、有无线行为、连接非法 WIFI、有无 4G 网卡、使用非法网关、连接外网和自定义外联等八种行为检查功能。当我们将设置好的策略下发至 PC 的准入客户端，准入客户端此时就开始发挥其作用。



安全入网后需要解决的另一个问题就是如何防止非法外联，AC 支持从外联检查和外联控制两个不同的层次加强对非法外联的管控，全面保障内网安全；支持的外联检测项包括：

◆ 拨号行为

拨号行为采用 RAS 远程访问服务完成，Windows 提供了一整套 RAS 远程访问服务的 API，通过调用 API RasEnumConnection 枚举出拨号行为，若拨号行为数量为 0 则表示本机没有拨号行为，反之则有拨号行为。

◆ 双网卡行为

通过读取 windows 系统汇总网卡存储的结构体获取网卡信息，然后通过网卡的 MAC 地址或者 IP 去判断多网卡的行为。

◆ 有无线网卡

通过 windows 系统 API 函数检测，判断无线网卡的数量，若数量大于 0 则代表 PC 上有无线网卡。

◆ 有 4G 网卡

先获取当前主机的所有网卡名（即 GUID），在注册表中判断对应的 ID 的值，若是以非 USB 开头的则为非 USB 外置网卡（包含无线网卡、2/3/4G 无线上网卡），若是 USB 开头的，则判断是否是无线网卡，如果不是，则为 2/3/4G 无线上网卡；

◆ 连接非法 WIFI

通过公司指定白名单 WIFI 上网的公司需检测是否连接的是非公司指定的 WIFI，可以通过 SSID 和 MAC 地址检测是否是非法外联，这个可以帮助网络管理员从 WIFI 源头管理上网终端连接 wifi 乱象。

◆ 连接非法网关

设置网关白名单，若本机网关在白名单上，则表示合法，否则表示非法。

◆ 连接外网

使用 ping 命令原理：内置 5 个域名，ping 通任意一个就判定链接了外网，每次只发一个包。

而外联控制则直接调用 windows 防火墙规则，实现非法外联强管控，严格禁止终端 PC 访问外网。外联控制的使用场景有如下两种：

■ 非法外联上报问题

当一个企业安装了安全软件且开启非法外联告警上报功能之后，各个部门区域都会上报非法外联告警，有的企业可能以此作为部门绩效考核的一项，我们知道，没有绝对的事情，例如测试部门为了测试就会不可避免的出现多次非法外联并上报告警，该部门的绩效就会收到影响。AC 提供的外联控制规则就能够效阻止此类安全软件上报非法外联告警，使部门或区域实现一定程度的自我管理。

■ 内网隔离

能够控制内网中终端 PC 可以访问的资源范围，实现网络中横向控制，切实的根据用户的需求场景保护网络中信息的安全。

3.2.2外设管控

各种各样的外设给我们的工作提供诸多方便，多一种途径就多一种方便，同样多一种途径也就多一分被攻击或中病毒的危险。AC 要做的就是解决被攻击和中毒的风险，向用户提供安全放心的网络环境。

◆ 配置外设管控的检查规则，添加到检查策略并下发至准入客户端，可有效管控如下类型外设：

存储设备 禁止终端使用便携式的存储设备，如 U 盘，手机，平板

网络设备 禁止终端外界网络设备，如移动数据网卡、无线 WIFI 网卡、蓝牙适配器共享网络、手机共享网络功能。

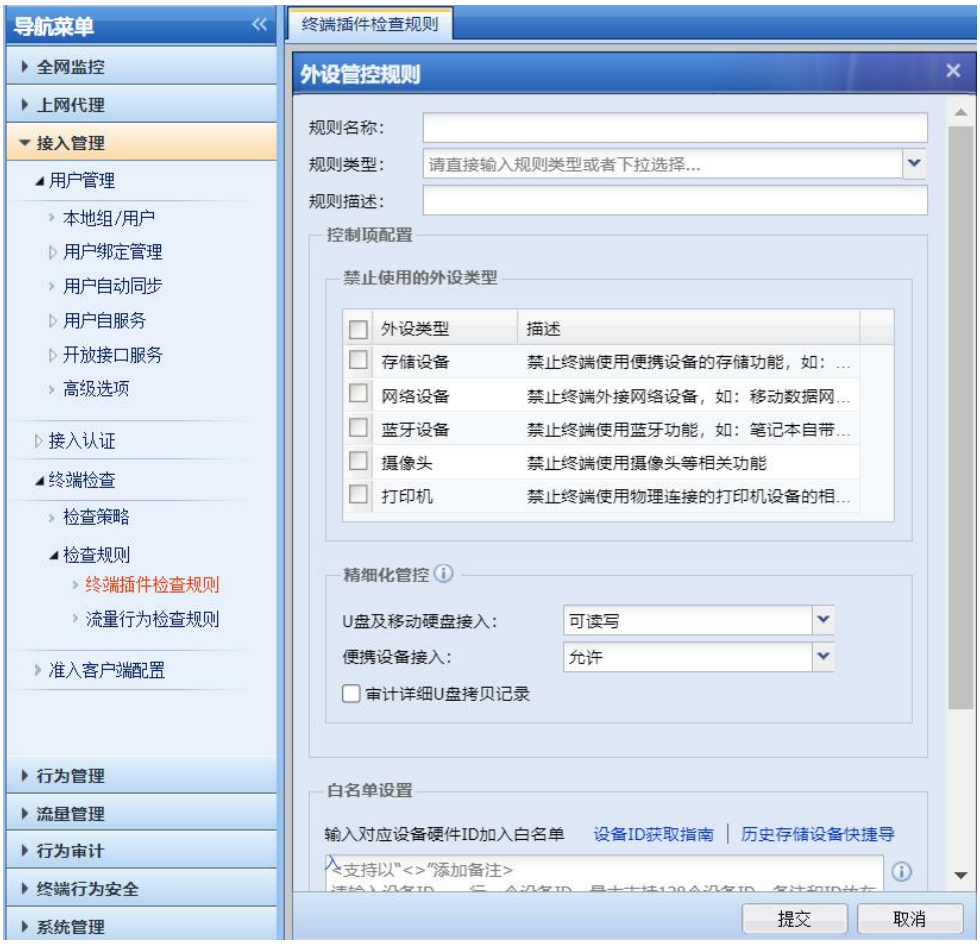
蓝牙设备 禁止终端使用蓝牙功能，如笔记本自带蓝牙、蓝牙适配器等相关功能。

摄像头 禁止终端使用摄像头等相关功能。

打印机 禁止终端使用物理连接的打印机设备等相关功能。

另外可处理的场景：

规则下发由准入客户端执行生效后，可以有效阻止监管程序上报非法外设接入的告警。



◆ 精细化管控

可以通过在 pc 端安装准入客户端，在 AC 端配置检查策略实现 U 盘及便携设备的精细化管控

支持控制动作有：

1、拒绝 --不允许使用 U 盘

2、只读 --允许使用 U 盘，但是不能向 U 盘写入内容（可以 copy 文件出来，

U 盘里打开文件）

3、可读写 --等同于不控制

4、告警 --对于 U 盘的插入进行告警

便携设备接入支持控制动作有

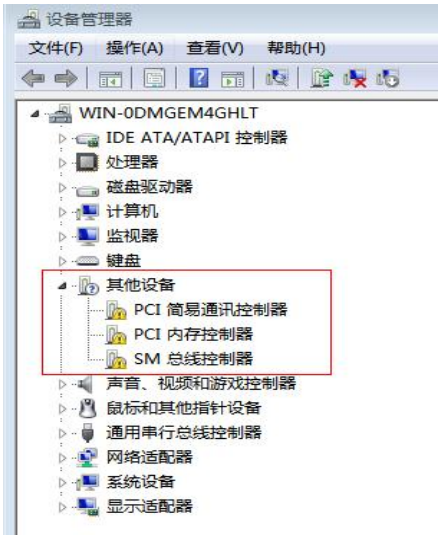
1、允许 --等同于不控制

2、禁用 --禁止接入

3、告警 --接入后进行告警

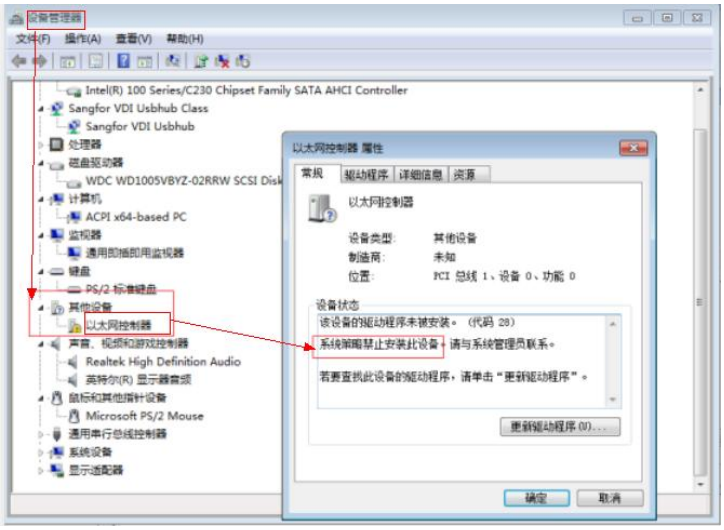
◆ 策略生效效果

当我们将设置的外设规则加入检查策略，并下发至终端，准入客户端每隔一段时间去查询是否有新的策略下发，检测到新的策略并使之生效，此时我们在 PC 终端插入未在设备 ID 白名单中的 U 盘，可以看到 U 盘被系统策略阻止了。



如何确定是由我们 AC 下发的外设管控策略阻止的，而不是由于终端设备硬件故障或 U 盘故障导致的呢？下图可为大家解惑：

右键单击 我的电脑——>管理——>系统工具——>设备管理器——>其他设备，可以看到提示“系统策略禁止安装设备，请与管理员联系”的字样。就说明是由于违反了系统策略导致设备安装失败，而不是硬件问题也不是系统问题。



◆ 原理

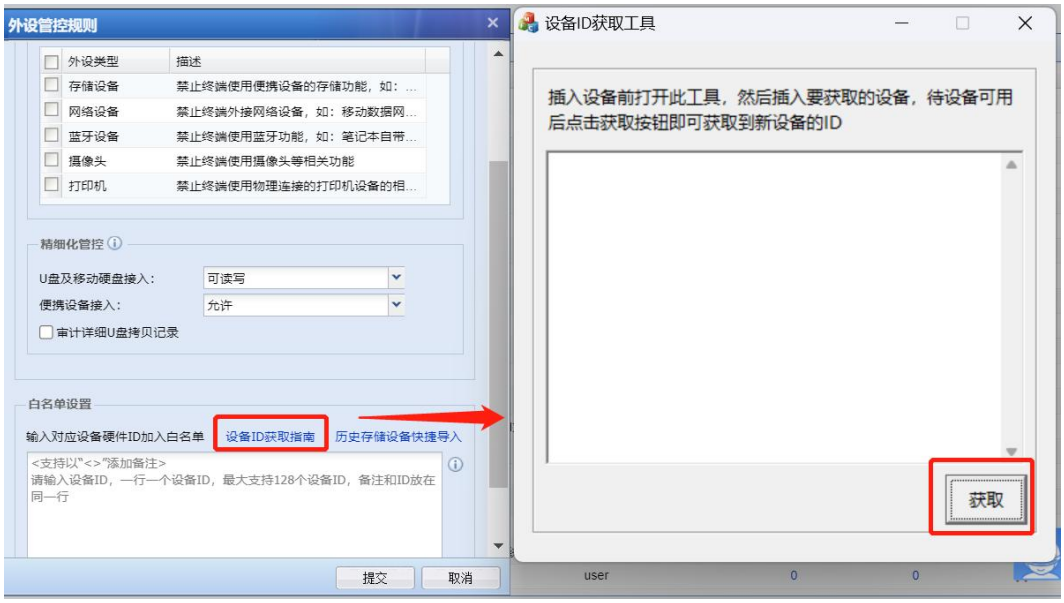
AC 下发准入策略，由准入客户端执行对应的系统脚本，相当于在 windows 系统（支持 win7 含 win7 以上版本）下手动设置系统组策略并生效。

◆ 设备 ID 生成

我们产品的目标之一就是给用户提供安全的网络，但不是只是安全确不方便，毕竟各种各样的外设确实是非常方便，但我们一味地禁止终端使用各种外设势必给用户造成多种不便，为了让用户能使用安全放心的外设，提供了外设白名单功能，即将一些指定、可信任的外设配置白名单，在白名单中的外设依然能够给用户提供各种便利，提供用户感受踏实的网络环境。

从 AC 下载生成工具并使用，操作步骤见下图：

管理员可以放通指定的外设设备，要用这个工具获取 ID 进行配置。



◆ 终端安全配置

这里我们需要重点关注的地方是手动找网关功能，该功能是我们在用户的使用场景中，根据实际需求提炼出来的，能够让检查策略更好的实施，该配置项的使用场景：

确保 PC 能找到网关

我们的准入客户端默认是自动找网关，这是一个比较复杂的过程，耗时且不一定准确，如果我们选择了指定网关，客户端下发之后就能准确的向指定网关发送各种业务的请求。

避免内网有多台 AC 的情况，找错网关

深信服有着二十年的历史，AC 的用户也可能是之前产品的用户，默认自动找网关的时候，也会出现找到之前产品作为网关，导致业务请求出错。

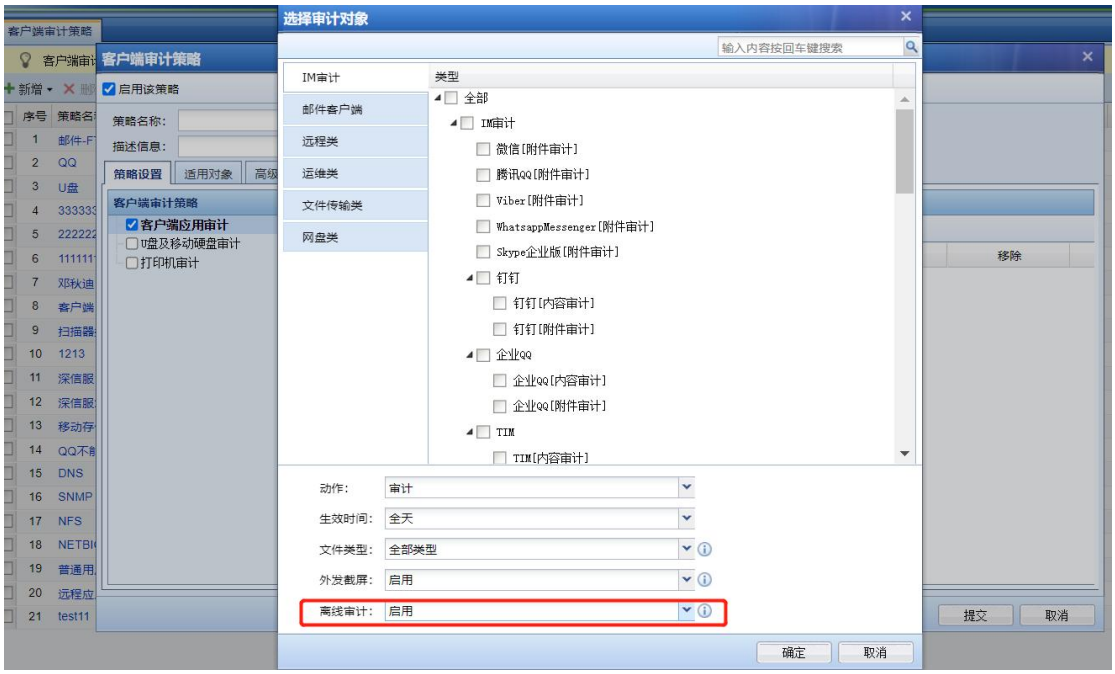
建议

最好均使用手动配置网关功能，可有效避免网关找不到或找错的情况。

3.2.3离线审计

为了解决移动办公，远程办公场景的审计需求，AC 支持准入客户端与设备连接断开的情况下实现离线审计，即使企业员工把笔记本带回家的情况，也可以实现 U 盘审计。

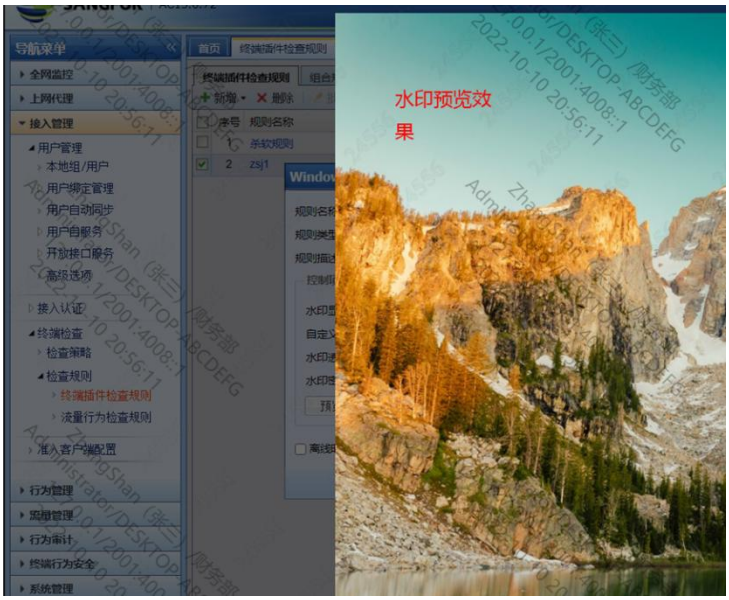
离线审计的原理：当准入启动以后无法连接到网关或者 2 分钟内未收到心跳包回包则切换至离线模式，如果此时缓存的策略文件打开了离线审计开关，则会继续记录 U 盘的文件操作：将要审计的目标文件备份起来，把行为记录到本地缓存，支持 1G 的最大缓存量，下次连上 ac 时上报到后台，在终端离线状态支持审计。



3.2.4 桌面水印

AC 准入客户端支持 windows 桌面水印，帮助客户提升敏感数据的管理，对敏感信息通过截图或拍照的方式外泄提供了一种溯源手段。

水印显示内容分为配置项和自定义内容，支持在控制台前端配置水印的透明度和密度，水印效果预览，并且终端离线时继续生效。

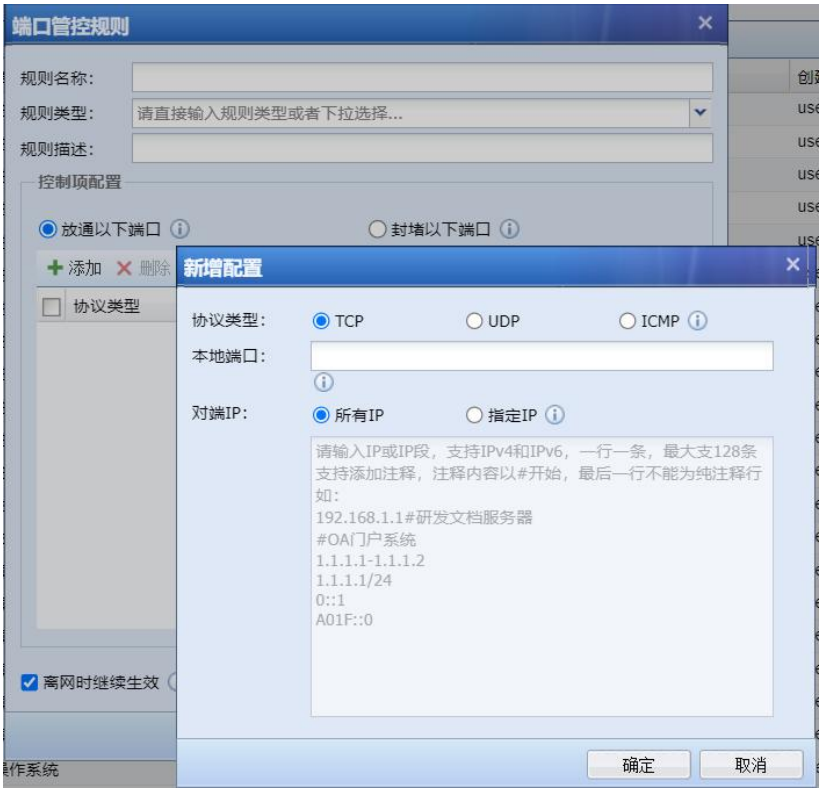


3.2.5 端口管控

在当前网络安全形势下，Windows 系统面临着各种安全威胁和攻击，高危漏洞的存在会给个人电脑带来严重的安全风险。因此，客户需要一种有力的管控方式，来保护个人电脑的

安全，防止恶意攻击和远程访问行为对个人隐私和数据造成的威胁。

对终端端口管控可以帮助客户更加有效地管控 Windows 高危漏洞，防止恶意攻击和远程访问行为对个人电脑造成的安全威胁。通过对指定的端口进行封堵或放通，可以实现对远程访问行为的管控，避免未经授权的访问和数据泄露等安全问题。



3.2.6 应用联网

一些应用程序可能会通过网络访问收集用户的个人信息，或者传输恶意代码进行攻击，从而对用户的隐私和安全造成威胁。通过控制应用程序的网络访问权限，可以避免这些恶意行为的发生，提高用户的安全性和隐私保护。

基于插件的应用联网控制功能可以帮助用户更加有效地管理应用程序的网络访问权限，从而提高网络安全性和隐私保护。

3.3 上网行为管理

3.3.1 身份认证

3.3.1.1 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；
- 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、用户密码+动态令牌认证；
- 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。

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。

3.3.1.2 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。

3.3.2 应用控制

3.3.2.1 应用控制策略

3.3.2.1.1 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 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：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。

3.3.2.1.2 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。

3.3.2.1.3 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。

3.3.2.1.4 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。

3.3.2.2 Web 应用控制

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+云系统”的识别体系。

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 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。

3.3.2.3 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 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，别有用心的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。

3.3.2.3.1 SSL 内容识别

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。

3.3.2.3.2 SSL 内容审计

AC 支持两种方式审计 SSL 加密的 WEB 网页、邮件、Windows 客户端应用的通讯内容，从而实现全面的上网行为可视和管控。

（1）中间人代理解密：AC 作为网关代理 PC 和服务器的 https 通信连接，通过证书替换方式解密 SSL 流量，终端访问 https 网页时连接实际上由 AC 的根证书进行加密验证。

（2）客户端代理解密：在准入客户端加上一个代理进程，通过操作系统驱动程序将数据包抓到代理程序，进而将经过 PC 的 TCP/UDP 流量都代理上，SSL 加密连接由客户端与服务器发起，通过代理进程将 SSL 解密 KEY 发送给 AC，流量实现代理后，在 AC 上进行 SSL 数据解密。

其中第二种方式需要在 PC 安装准入客户端，该方式解密性能大幅度优于传统中间人解密，且避免由于替换证书造成的网页告警，实现高性能、无感知的解密审计。

3.3.2.4 共享上网控制

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。

3.3.2.5 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，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。

3.3.3 带宽管理

3.3.3.1 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。

3.3.3.2 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。

3.3.3.2.1 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。

3.3.3.2.2 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。

3.3.3.2.3 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。

3.3.3.2.4 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。

3.3.3.2.5 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。

3.3.3.2.6 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。

3.3.3.2.7 应用引流和智能负载

AC 采用应用路由技术、DNS 透明代理技术以及链路繁忙控制等技术实现基于链路的负荷情况、时间段、用户群体、访问对象等因素来分配链路的分配机制，进一步提升链路优化使用率。

AC 支持按照终端用户群体、上网应用、访问域名、源地址段、目的地址段、传输协议、IP 层 DSCP/TOS 标记等因素来设置引流范围，支持动态负载（优先使用高优先级线路）、指定线路、按运营商负载、按线路带宽负载、按剩余带宽负载、VPN 做专线备份等多种负载方式，提升引流效果。采用动态引流技术，优质线路空闲时其他用户和流量也可以跑优质线路，优质线路快要繁忙时，引走非核心应用流量和非核心用户流量，在保障核心用户和核心应用的上网体验前提下，对优质线路充分利用，避免空置浪费。

3.3.4 行为审计

3.3.4.1 WEB 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、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。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。

3.3.4.2 客户端应用审计

PC 客户端应用大多采用加密协议，包括 SSL 加密和私有泄密加密，对加密客户端内容的审计一直是业界上网审计的最大挑战之一，AC 通过创新方式实现常用客户端审计。

（1）客户端代理解密（同 SSL 内容管理）

在准入客户端加上一个代理进程，通过操作系统驱动程序将数据包抓到代理程序，进而将经过 PC 的 TCP/UDP 流量都代理上，通过代理进程将 SSL 解密 KEY 发送给 AC，流量实现代理后，在 AC 上进行 SSL 数据解密。终端代理程序是跨平台的，将应用层与驱动层分离。针对市面主要浏览器做默认代理，支持范围广。

（2）应用外发附件审计

采用消息钩子注入的方式对 windows 系统函数做注入处理，可以审计到多种上传附件的操作，是对客户端外发文件审计的通用方案，通过简单修改规则，就可以增加对应用的支持。AC 目前支持多款常见运维工具、网盘/笔记类应用、FTP 应用、远程控制应用的外发附件审计。

（3）U 盘审计

支持 U 盘和移动硬盘拷贝的文件内容以及插入和拔出行为的审计。

（4）打印机审计

支持 Windows 终端（win7/win8/win8.1/win 10/win11）打印文件行为和打印文件内容的审计。

3.3.4.3 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、关键字搜索、论坛微博搜索等

- 趋势：流量趋势、行为趋势、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；

3.3.4.4 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。

3.3.5 上网代理

3.3.5.1 HTTP、SOCKS 代理

代理是一种特殊的网络服务，允许一个网络终端（一般为客户端）通过这个服务与另一个网络终端（一般为服务器）进行非直接的连接。一般认为代理服务有利于保障网络终端的隐私和安全，防止攻击。AC 支持 HTTP 代理和 SOCKS 代理，包括 HTTP、SOCKS4、SOCK5 代理数据基于源 IP 地址和目标主机的权限控制；持对代理流量进行二次分类，有效识别访问网站、web 流媒体、在线炒股、网络游戏等各种应用，并基于用户、时间等条件灵活管控，以保障客户关键业务服务质量。

3.3.5.2 ICAP 协议支持

ICAP，即 Internet Content Adaptation Protocol，本质上是在 HTTP message 上执 行 RPC 远程过程调用的一种轻量级的协议。通过 ICAP 可以将 HTTP message 发送到 ICAP 服务器进行内容检查。

AC 支持实现 ICAP 的请求修改协议，与第三方的 ICAP 服务器进行对接。使用代理时将 http 数据发送到 ICAP 服务器进行检查（恶意软件、DLP 等）。如果检查通过，ICAP 服务器会将原数据返回，继续到 PC 或 WEB 服务器。如果检查不通过，则将会把检查结果发送到 PC

端展示。

3.3.6 安全防护

3.3.6.1 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。

3.3.6.1.1 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。

3.3.6.1.2 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。

3.3.6.1.3 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。

3.3.6.2 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。

3.3.6.3 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 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。

3.4 业务行为审计

3.4.1概述

随着企业信息化的发展，内部业务系统越来越多，业务系统上数据越来越多：

1. 业务系统梳理困难的问题。企业内部有很多系统，由于历史的原因，很难对业务系统进行梳理，难以对资产进行有效管理，导致存在很多安全隐患。

2. 业务系统访问的留存和追溯。企业的重要数据大都在各业务系统上，因此对业务系统的访问要进行日志留存，以便后续发生事件可以进行追溯。

3. 账号安全管理。业务系统使用的问题很多是由于账号的不当使用引起的，特别是在重要的业务系统里，由于账号的不合理使用导致了很多安全隐患。

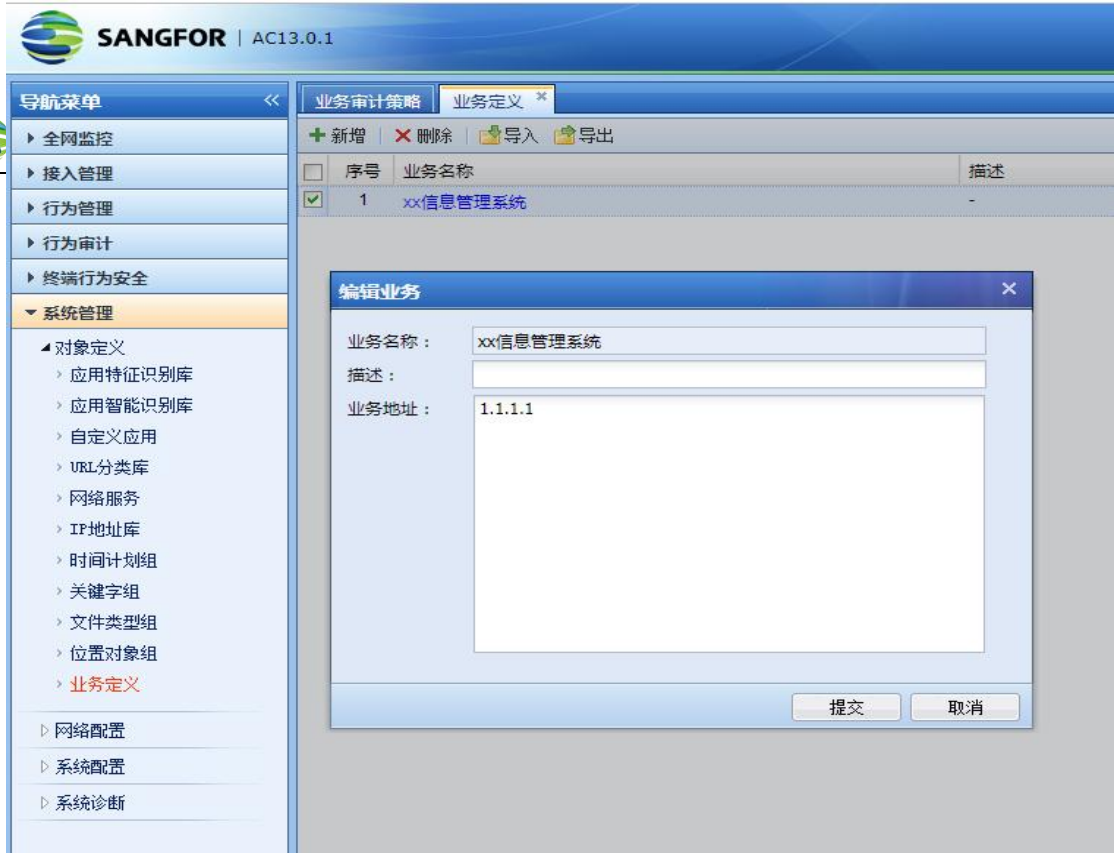
AC 在互联网审计和业务审计（提供了应用审计、流量和上网时长、网页内容审计）、日志记录、报表分心等不同层级的全面行为审计。实现用户网络的全面管控，不仅支持互联网侧的行为审计，同时支持内网侧的行为审计，可以让用户对自己的网络行为有更多更全的管理监测方式。

3.4.2实现方式

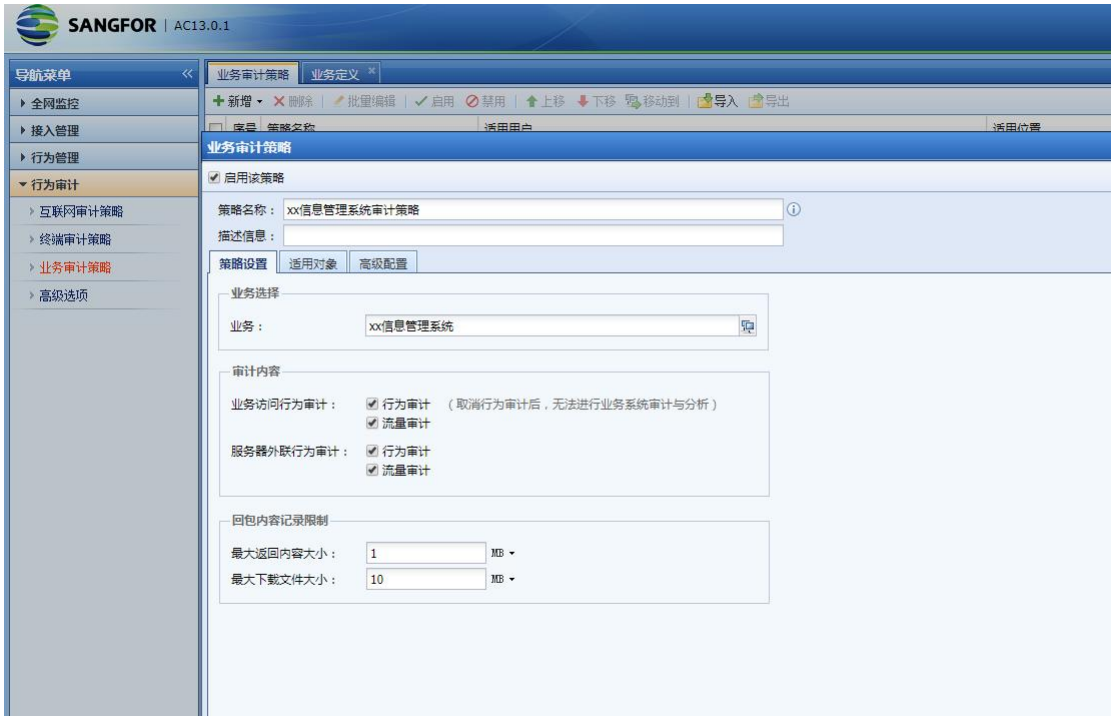
AC 支持通过镜像流量，指定 IP 范围，即可自动识别业务和协议，自动审计；自动区分业务访问和业务外联行为和流量分别审计。
Tcp 流量经过业务系统识别模块，识别为业务系统流量，应用审计模块把 tcp 流量组装成 http 协议单元，业务审计插件把 http 协议单元记录成日志。分为两种日志类型。业务外联日志：指业务主动连接外网产生的日志；业务访问日志：指用户主动访问业务产生的日志。审计对象包括：服务器：指物理服务器；业务：指服务器上对外开放的业务，一个服务器可能有多个业务；用户：访问业务的人。

3.4.3业务审计

AC 支持自动识别业务和协议。管理员需指定业务 IP 范围，系统即可自动识别开放的业务端口，里面的流量类型，并自动记录日志；通过指定 IP 范围自动识别内网业务系统，客户端访问目的地址即使业务系统。



审计内容包括业务访问行为审计和服务器外联行为审计，并且记录回包内容。



4 产品核心价值

4.1 终端入网管控

从终端入网开始，深信服全网行为管理 AC 对接入终端进行高精准度资产识别，提供 802.1x、Portal 等多种身份认证方式，同时进行终端安全基线检查、终端外设权限管控，

帮助用户建立终端入网安全规范，降低安全隐患和数据泄露风险。

4.2 上网行为管控

对于入网后的终端，深信服全网行为管理 AC 基于海量级 URL 库和应用规则库，实现应用细分动作控制，同时做到全面无疏漏的合规审计，支持动态流控、应用引流等技术，实现带宽分配合理，帮助用户保障上网规范和上网体验，避免违法违规。

4.3 终端行为管控

轻量级桌面管控：端口管控、应用联网管控、软件安装管理、屏幕水印、外联管控、外设管控，帮助管理员更好地管理和控制用户的终端行为，从而提高系统的安全性。深信服全网行为管理 AC 创新网端一体化管控，让办公更规范、更高效、更安全。

5 产品特点与技术优势

5.1 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。

5.2 SSL 终端解密

AC 可以利用轻量级插件，需做中间人代理，直接跳过非对称的握手计算过程，只进行对称加解密运算，实现 SSL 解密。通过在终端 PC 安装客户端，客户端获取终端应用与服务器 SSL 连接握手信息发送给 AC 设备，则直接解密和加密该 SSL 连接的上下行数据包，达到审计和控制效果。

该方案有提升系统吞吐率；可以实现全部署（旁路、路由、网桥）对 SSL 协议数据进行审计和控制；部署简单，硬件成本低；浏览器中的网站证书无告警等优势。

5.3 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。

5.4 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。

5.5 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员的身份，避免行为日志被滥用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 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。

5.6 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。

6 产品部署模式

6.1 网关部署

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：

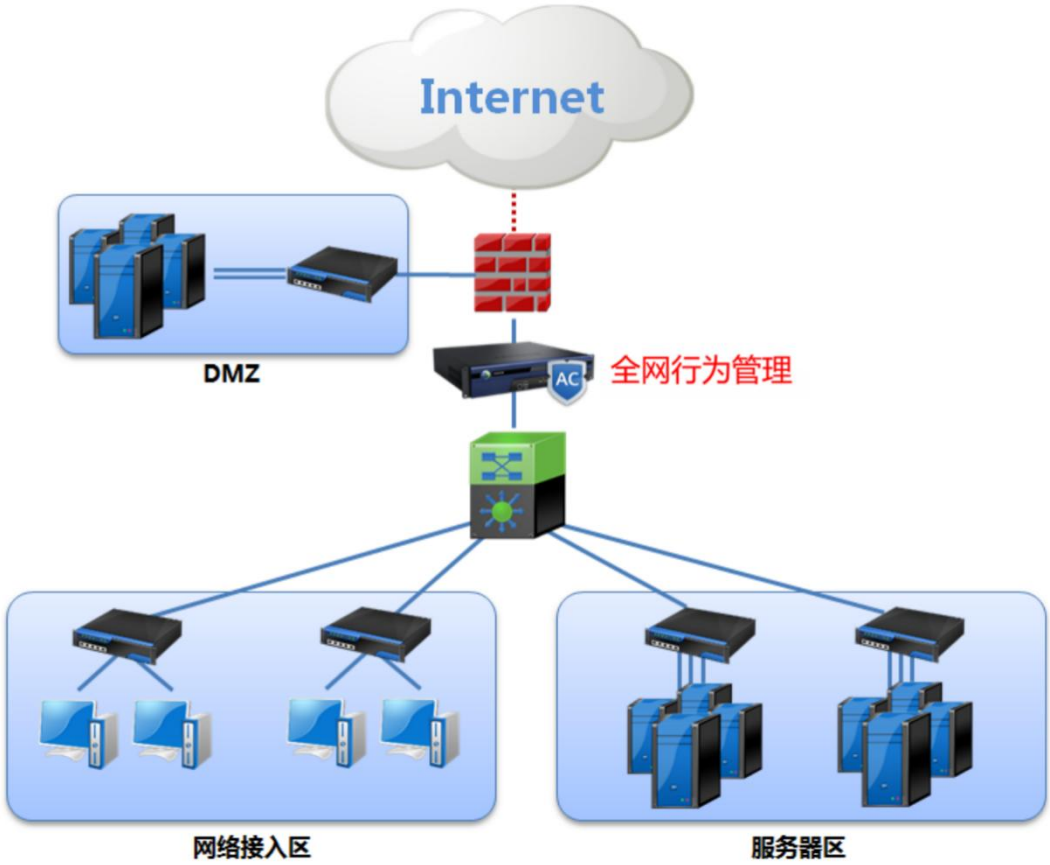
1. AC 的 WAN 口与广域网接入线路相连，支持光纤、ADSL 线路或者是路由器；
2. AC 的 LAN 口（DMZ 口）同局域网的交换机相连；
3. 内网 PC 将网关指向 AC 的局域网接口，通过 AC 代理上网。

6.2 网桥部署

6.2.1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。

6.2.2多网桥模式

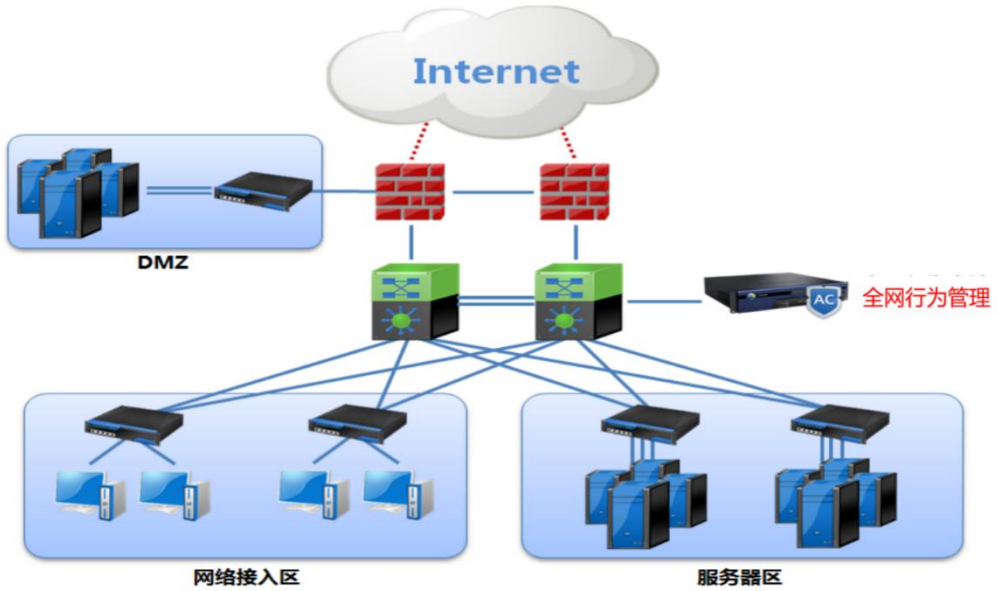
组织考虑到网络的稳定性、可靠性，往往采用双机、双线路构建基础网络。AC 支持多路桥接模式，适应组织的多机网络环境要求。在不影响原有双机、双线路前提下，对流经 AC 的所有数据流进行审计、控制、拦截、流量管理等操作。

部署方式：

1）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。

6.3 旁路部署

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。

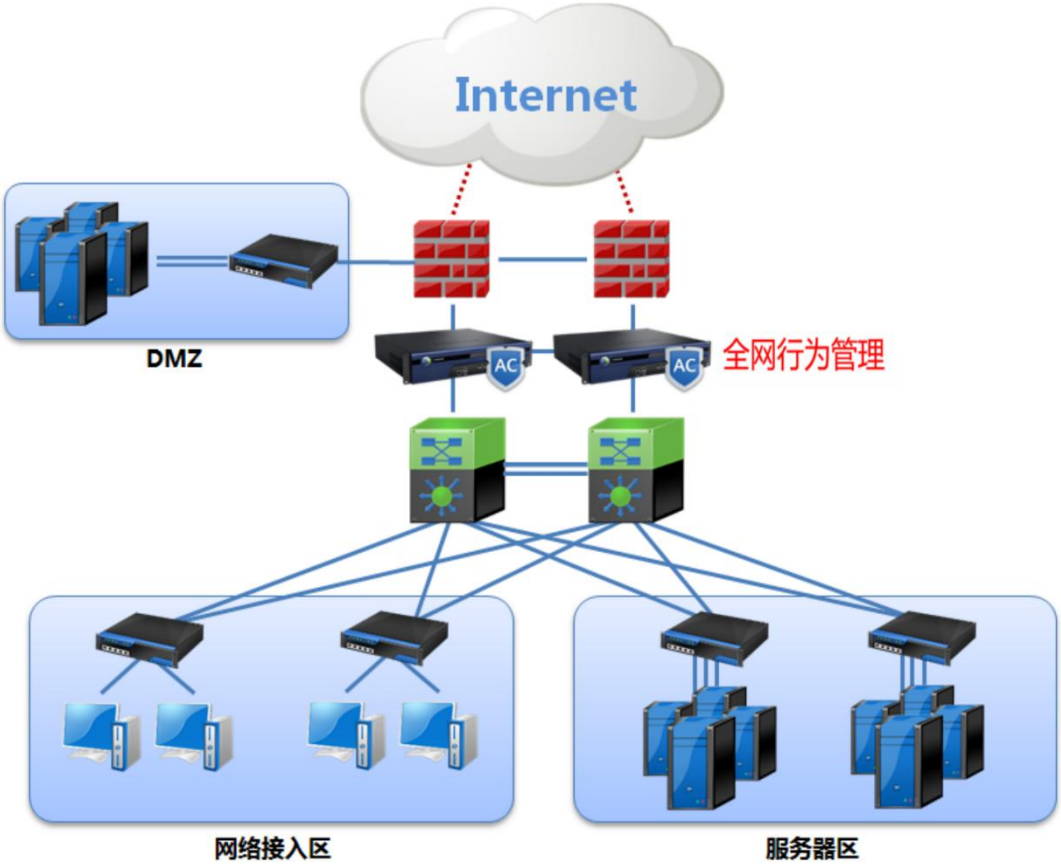


部署方式：

- 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。

6.4 多机部署

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。

6.5 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。

7 关于深信服介绍

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 2018 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。

将产品和服务做到最好，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、全网行为管理 AC、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、全网行为管理 AC、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。