某人民政府政务服务中心
解决方案

安徽云图信息技术有限公司

目　录

项目基本信息

项目名称	某人民政府政务中心解决方案
客户方	某人民政府
支持方	安徽云图信息技术有限公司

1、项目背景

1.1 项目背景

某人民政府政务服务中心为某县政府直属正科级工作部门。中心设立党的工作委员会，为某县委工作机构。县政务服务中心设主任一名，副主任两名，内设综合科、督查科。中心定编八人，现有正式在编在岗工作人员八人，调研员一人，聘用五人。

中心现有窗口单位 30 个，工作人员 72 名。其中，党员 33 名，占总人数的 39%。2011 年 8 月，在原先机关党支部基础上，增设县政务服务中心政务服务大厅第一党支部和第二党支部，将窗口所有党员统一纳入中心管理。

1.2 项目现状

某人民政府政务服务中心现有带宽 20M，上网用户 70 人左右。内部上网没有专业的上网行为设备作为审计，网上办公没有对相关上网人员上班时间做与工作无关的事做任何限制，严重影响内网用户正常办公。

1.3 项目需求

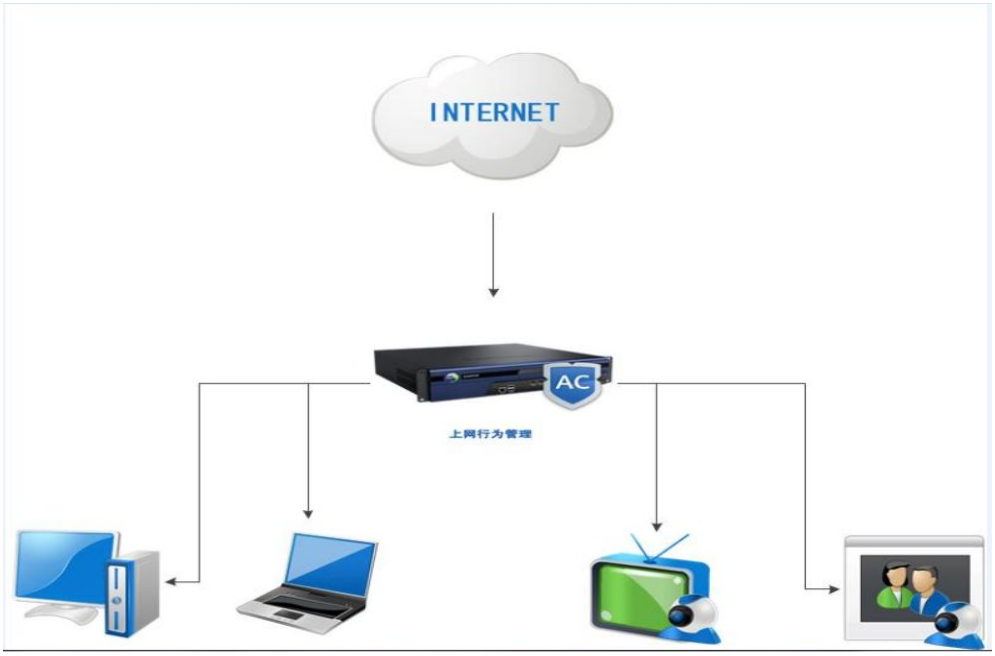
目前政务服务中心需要以下几方面功能：1）控制非工作行为和流量，保证业务数据的流畅。单位用管控功能来控制非工作的行为和流量，如特定网站、游戏、聊天、炒股、音视频等，以便维持网络的正常使用和运转。防止出现某员工的某种行为过多占用公司带宽的情况。2）对各种网络行为进行细粒度的记录，以便了解员工的每一个上网行为细节，存档备查。3）发现上网规律、预见员工面临的困难和风险，并且采取相应措施协助员工解决。对各种上网行为进行细致、深入的归纳和分析，总结出规律和风险，根据不同行业的特点形成主题报表向领导呈现。

1.4 项目目标及意义

通过采购、安装、配置上网行为管理网关、及相关网络互联设备，在网络出口处部署上网行为管理设备，使互联网访问数据受到监控，阻止有害的外发信息；对互联网访问行为进行记录和控制，封堵或减少内网用户使用 QQ，网上购物，网上炒股，大流量下载等行为，对带宽进行合理有效分配；对内网单机的安全措施做有效管理。从整体上实现公司 IT 业务高效率，无故障运转。

2、解决方案

根据用户需求，我们制作了宏观的拓扑示意图：



该拓扑大致表明了 AC 的上网管控模式及位置；

3、AC 给用户带来的价值

深信服科技（SINFOR）的 AC 产品带来了全面而细致的互联网行为管理解决方案。在此，我们通过对 AC 在管理网络带宽、保障内网安全、提高生产效率和规避法律风险这四个方面来具体阐述其为用户带来的商用价值。

2.1）网络资源的维护与管理提升

通过全面的网络使用情况的日志，统计报表，IT 部门可以全方位掌控内网。避免以往对内网情况无从可知的情况。网络资源的维护与管理程度可以大幅提升。

2.2）提高内网安全

通过对内网单机进行全面安全检查，减少内部漏洞，得以全面防范病毒及木马入侵可以降低由此带来的资料损失，硬件破坏等.

2.3）提高生产效率

以每位员工平均每日在网上消耗的非工作时数 1 小时的保守估计，上网行为管理提升工作效率可达 14%。而通过提升带宽利用率，保证重要的业务带宽不被占用，更大程度提高工作效率。整体而言，预计可提升工作效率 20~40%左右。

2.4）规避法律风险

为防止内部人员访问一些非法的网站和论坛，可通过 URL 过滤和阻拦，设置关键字过滤等手段。对于内部人员所访问的网站进行完全的记录，包括具体的访问时间，登陆地址等。为防止内部人员通过 IM 软件传送一些机密信息，可以实现对 IM 软件的完全封堵或者完全监控和内容记录。为做到有据可寻，通过日志中心，对所有人员上网行为做一个完全记录，方便信息部对整个网络访问流量有一个量化的认识，使系统管理员更好得维护和管理网络。

4、 设备介绍

4.1 有效进行部门规划

首先根据职能部门来划分用户组。有些部门由于物理环境的限制无法获取连续的 C 类地址，但这不会影响 AC 的使用，只需要继续添加。对于某些不属于特定部门的人群，可以另外建组。

4.2 建立身份认证体系

3A（认证，授权和审计）是组织安全基础设施的基础，将对用户和内容进行有效的保护和控制。基于内网的安全的认证机制还需要进一步完善，需要管理局域网中所有用户的 Internet 访问。

身份认证主要有两种方式，免客户端认证和客户端认证，AC 中的 Web 认证属于前者。Web 认证通过浏览器即可完成全部认证，即使对计算机操作并不熟悉的用户也能够理解和操作，很好提高了操作的互动性和弹性。

AC 支持多种认证方式，除了通过用户名/密码、IP/Mac 认证外， AC 的 Web 认证还可以透明结合 Radius、LDAP、POP3 等认证服务系统进行用户身份校验。IP/Mac 认证可以通过 AC 自带的局域网扫描功能实现。对于后几种认证手段，只要在 AC 中正确填入域、活动目录和邮件服务器的地址和端口，AC 将自动更新用户列表和策略，这对建立了完善的内网认证体系的用户非常方便。

4.3 开始分析网络流量

当用户通过认证系统的身份校验后，AC 将为不同的用户组进行授权，将系统管理员设定的策略同用户的标识相对应。在 AC 中，这些规则的制定主要从保护、控制和监控出发，并将这些规则和用户有机地结合在一起，进而形成一套完整的访问控制策略。

当局域网中的用户通过了认证、授权后，你往往要面临严峻的广域网带宽使用问题。好的改变方法是部署基于广域网的加速设备。

AC 的网络数据中心（Network Data Center， NDC）是一种统计分析工具，它可以记录局域网用户访问 Internet 的所有流量。

4.4 优化带宽资源

在不能改变狭窄带宽的前提下，需要去适应带宽，进而优化带宽。

首先可以考虑使用 AC 的 QOS 和带宽叠加功能 ,AC 将对广域网的带宽优化起到有效作用。QOS 的设定有助于那些要求高传输质量、低时延的服务取得优先的带宽。

而带宽叠加技术作为深信服科技的一项专利（专利号：200310112006X），已被直接用在 AC 上网行为管理这条产品线了。通过绑定多条 ADSL 或专线，可以获得更大的出口带宽，当多条 ADSL 绑定时，可以获得超过单条 FTTX 的带宽，而其费用却远远低于后者。这对于拨号和 xDSL 资费低廉而且专线线路难以申请的地区尤其有吸引力。、

更具效力的网络流量优化方式是 AC 的基于用户的流量控制技术 (User - Based Traffic Control, UBTC）。在广域网的访问中，有些部门的特殊应用是应该而且必须获得独占性资源的，而有些部门的非工作相关服务本不应获得更高的带宽。通过 AC 的分组流量控制,可以对不同用户组使用的服务进行精细到以 K/Bps 为单位的带宽分配，保障重要部门的重要服务得到足够带宽，使非重要的服务受到合理的流量限制。

当管理员对互联网的使用情况有了大致的了解后 ,可以针对用户组的行为做出进一步的管理和控制。

4.5 网页浏览的控制

网页的浏览是互联网访问的主要内容。一方面，组织的管理者不希望给办公室营造监狱一样的环境，为了使员工得到更好的心情和满意度，组织需要一个人性化的环境。另一方面，员工对互联网的滥用的确带来了严重的生产力流失。

在 AC 的内置库中有着数百万的 URL 资料，分为新闻、音乐、视频、成人、财经、教育、科技等条目。在局域网中的用户浏览网页时，AC 的联动式分析系统（Link Analysis System, LAS）将发挥作用。通过 LAS 技术，AC 将根据网页的内容、用户可管理的关键字组、网页中包含的文件类型进行联动式分析，并根据 AC 默认的设置、管理员自定义的过滤规则对用户需要访问的网页进行过滤。

同时，AC 还可根据工作时间，季节等最时间进行兼具计划性和灵活性的划分。

4.6 管理即时通讯工具

不断成长壮大的 IM 已经成为了事实上的企业通讯标准。 然而，IM 的大量使用也造成了生产力的流失和机要信息的泄露。

AC 可以提供对 IM 软件从禁止、监管、再到安全性审查的解决方法。

4.7 应对 BT 类软件

P2P 技术对带宽资源的争用使局域网有限的带宽被耗尽， P2P 的封堵应该是所有安全网关都需要关注的问题。

AC 可提供两种封堵方法，一种是基于应用协议和数据包的分析，另一种是针对流量进行检测。首先，AC 的深度内容检测服务（Thorough Content Detection, TCD）可以对 BT 类应用的数据包进行深入检测。TCD 通过分析 IP 数据包首部的服务类型、协议、源地址、目的地址以及数据包的数据部分，实现了从四层到七层的全面内容检测，能够更好的发现哪些服务是 P2P 类应用，而不再使封堵仅限于对端口的分析和封锁。

由于 TCD 技术将对数据包进行深入分析，当内网用户发出的会话较多时，网关设备也将花费较多的资源来处理更多的数据包。为了避免大量的数据包分析带来的资源消耗， AC 采用了网络流量智能分析技术(Network Traffic Intelligence Analysis，NTIA）。区别于端口封堵和内容检测，NTIA 技术将对每一个用户和用户组的网络连接情况进行分析，当网络流量和网络连接超出 AC 规定的阀值时，用户的 P2P 行为将被限制流量。

一些 P2P 封堵技术实现了对某些 BT 类应用的“杜绝”，例如 Cisco 采用的 NBAR，NBAR 将对 BT 和电骡产生的数据包丢弃而不是管理 ,但更理想的方式应该是合理的利用 P2P 技术为我们的资源共享服务。上面提到的深度内容检测（TCD）和网络流量智能分析（NTIA）都能够提供给用户更多的选择。当 AC 确认某些用户在下载 P2P 文件时，网管员可以采取三种策略，首先是允许下载，这是对 VIP 和紧急用户的特权选项；其次是拒绝，你可以选择对某项 P2P 服务彻底封堵；最后是流量控制，即内网的用户可以使用 P2P 类软件，但他们产生的流量和连接能够被控制在一个可以接受的范围之内。

4.8 控制其他的网络应用

Internet 上的网络行为还远远不止以上提到的内容。需要管理者关注的还有网络游戏、在线视频（MMS、HTTP Streaming、RTSP 等）、在线炒股等应用。

AC 的深度内容检测（TCD）已经自带了众多应用程序的数据特征文件，通过对用户组的访问控制设定，你可以轻易地允许或者拒绝内网用户访问特定的网络服务。作为一种面向客户的开放式解决方案，AC 提供给用户更丰富的自定义功能。在 TCD 的高级设置中，AC 允许有编程基础的网络管理员添加、修改和导入自定义的网络应用规则。如果局域网内有人使用非公开工具进行不正当活动，通过分析其工具的数据内容，AC 同样可以实现封堵和控制。

4.9 防止机密泄露

在 FTP 的防护措施上， AC 可以通过关键字和文件类型的设定来限制 FTP 的传输内容，对于内

网通过 FTP 上传到公网的内容，AC 将进行记录和保存，以便更好的对违规、违法员工进行网络行为追踪，进而更好的保护组织资产。

在邮件的发送中，AC 可以启用邮件延迟审计（Postponed Sending after Audit，PSA）,通过 PSA 技术，内网的邮件将收到更为细致和全面的审查，以避免机密信息的不慎或有意泄露。具体内容您可以参考下一章的“邮件延迟审计技术”介绍。

BBS 的访问主要分为 Web 登录和 Telnet 登录，对于 Web 方式的访问，AC 同样可以通过对关键字的审计来限制内网用户的发帖行为；而对于 Telnet 方式的登录，AC 亦可以记录命令的详细内容，以供后期的审查使用。

4.10 更多的安全机制

VPN/防火墙

反垃圾邮件

入侵防御系统

防 DOS 攻击系统

网关杀毒

5、 部署方式

作为保护组织网络资源的核心设备，AC 考虑到了各种可能的网络拓扑，并力求部署的最简化。

穿透式（Pass-Through）部署

穿透式部署将设备部署在局域网的主干部分以处理流经设备的数据流

网关（Gateway）模式

网关模式适用于希望通过 AC 产品来实现所有的审计、控制和拦截功能，且对网络

拓扑的更改不敏感的用户。

网关模式将 SINFOR AC 作为局域网的出口网代理内网 PC 上网，除完成 AC 的管理控制功能外还可以实现 NAT、路由和防火墙等网络与安全功能。

部署方式：AC 的 WAN 口与广域网的接入线路相连，一般是光纤、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，内网的 PC 将网关指向 AC 的局域网口，进而通过 AC 代理上网。

网桥（Bridge）模式

网桥模式适用于希望对内网完全监控、控制和管理，且不希望更改局域网的任何网络地址的用户。

网桥模式将 SINFOR AC 等同于一根连接在网关和交换机之间的“智能网线”，可以对所有流经 AC 的数据流进行审计、管理和控制。

部署方式：AC 的 WAN 口同局域网的网关相连，LAN 口（DMZ 口）同局域网交换机连接。局域网内的任何网络设备和 PC 都不需要更改 IP 地址。

旁路式（Pass-by）部署

旁路式部署将设备与交换机的镜像口相连，用于监听局域网中的数据流

旁路（Pass - by）模式

旁路模式适用于希望通过 AC 来实现内网监控和审计的用户。

旁路模式的部署不需要对内网拓扑作任何改动，使实施难度最低。而由于内网数据流不需要流经 AC 设备，避免了网络主干中设备过多引发的网络处理性能下降，也降低了网络单点故障的发生几率。

部署方式：在出口交换机中配置镜像端口，将 AC 的广域网口同镜像端口相连，实现对内网数据包的监听。