工程管理
Journal of Project Management
第 6 卷◆第 8 期◆版本 1.0◆2025 年
文章类型：论文| 刊号（ISSN）：2737-4580(P) / 2737-4599(O)

公司上网行为管理系统建设方案浅析

官小琦
中石化石油工程设计有限公司
DOI:10.12238/jpm.v6i8.8337

[摘　要] 随着互联网时代的到来，各种网络应用层出不穷，对目前我公司的互联网管理带来的巨大挑战，传统的基于 IP 和端口管理方式已经无法满足管理精细化的要求，因此公司上网行为管理系统的建设已经成为了网络管理的迫切要求。本文通过分析目前网络管理中的问题，针对性的提出了上网行为管理系统建设的目标，方案和功能，为系统建设提供了参考和借鉴。

[关键词] 互联网；行为管理；流量控制；内容审计

A Brief Analysis of the Construction Plan for the Company's Internet Behavior Management System

Guan Xiaoqi

Sinopec Petroleum Engineering Design Co., Ltd.

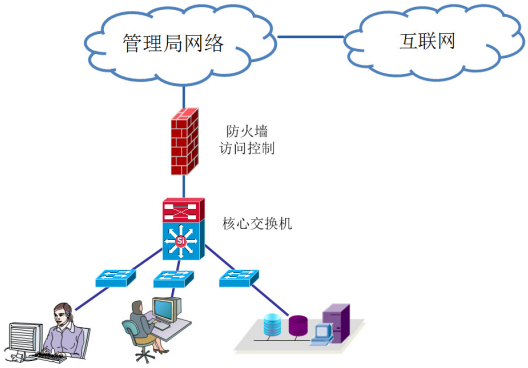
[Abstract] With the advent of the Internet era, various network applications emerge in endlessly, which brings great challenges to our company's Internet management at present. The traditional IP based and port based management methods can no longer meet the requirements of refined management, so the construction of the company's online behavior management system has become an urgent requirement for network management. This article analyzes the current problems in network management and proposes targeted goals, solutions, and functions for the construction of an online behavior management system, providing reference and inspiration for system construction.

[Key words] Internet; Behavior management; Flow control; Content audit

随着信息技术的深入发展，互联网日益成为人们工作、学习和生活的一部分。在享受互联网带来的巨大便利的同时，由其带来的负面影响和安全威胁也日趋严重；复杂的互联网使用环境引发了诸多问题，诸如组织成员工作效率降低、带宽资源滥用、信息机密外泄等问题，并因此而产生法律、安全、组织名誉以及组织公信力等问题。因此，加强互联网访问管理、规范上网行为、提高网络利用效率已成为当务之急。

1.公司互联网使用现状

我公司的局域网是胜利石油管理局信息网的一部分，没有本单位独立的互联网出口，所有互联网的访问都通过管理局的外网出口。公司核心交换机通过防火墙接入到管理局网络中。防火墙的主要作用是对通过访问控制策略，动态阻断 IP 用户非法访问并放行合规流量，实现内网资产与外部威胁的安全隔离。目前公司网络出口设备连接情况如下图所示。



公司目前的互联网访问主要是基于三层 IP 地址和应用层端口的管理方式。对不同类型、不同级别的人员分层次进行管理。

2.互联网使用中存在的问题

目前公司的互联网管理只是基于防火墙的访问控制管理。管理策略主要是基于 IP 地址和协议端口设置。随着互联网技术和应用的不断发展，该设备无法识别各种网络威胁和限制各种资源占用率较大的应用，无法满足对网络使用精细化、个性化、安全化管理的要求，无法保证网络访问的合法性和高效率。

目前公司互联网使用过程中主要存在以下问题。

（1）工作效率降低。很多具备访问互联网条件的员工热衷于网上购物、炒股、游戏、在线视频等各种与工作无关的应用，占用了大量的工作时间，严重影响了日常工作效率。

（2）网络带宽利用率低，访问速度慢。管理局目前的互联网出口带宽较小，使用人数较多，客观上决定了我公司目前互联网访问速度慢。但是目前网内各种迅雷、BT、在线影视娱乐等各种 P2P 下载功能的使用也占据了大量的网络带宽，造成带宽利用率低，影响了公司正常业务对互联网的使用。

（3）存在机密信息外泄可能。目前公司互联网缺乏安全管控，造成公司很多机密文件和重要资料可能通过微信、钉钉、QQ 等途径外泄。员工不当的互联网使用行为也会造成计算机感染木马病毒造成资料被他人截取。

（4）病毒和木马泛滥，可能导致网络瘫痪。高风险网站导致病毒、木马、流氓软件在内网散播，造成无法正常的使用网络。用户随意下载的非正规软件等已成为病毒、木马、蠕虫、间谍软件的重要传播渠道。目前公司在这些方面缺乏有效的管控手段。

（5）不当的应用，存在潜在的法律风险。员工使用公司局域网进行非法的互联网访问，非法 P2P 内容下载，传播不健康信息，发表不当言论，均会对公司和组织造成潜在法律风险。

3.系统建设的目标

目前我公司互联网访问中存在的各种问题，要求我们尽快建立公司的上网行为管理系统，加强网络应用管理，控制非法访问和接入，提高网络安全性，保障业务应用，实现互联网使用的精细化管理。

公司上网行为管理系统的建设目标分为管理方面目标和技术方面的目标。

管理方面的目标：

（1）系统不改变目前公司网络的管理方法和模式，不影响公司目前对互联网权限的访问控制。

（2）系统能够根据不同用户的需要，灵活方便的制定个性化的管理策略，满足各种形式的管理级别和要求。实现不同用户、不同时间、不同应用的多维度管理。

（3）避免系统造成的用户端的插件安装或者其它操作和设置，减少系统部署后员工对系统的抵触情绪。

技术方面的目标：

（1）系统不改变公司网络现有的架构，仅对互联网使用进行管理，不对油田局域网和公司内部业务应用造成任何影响。

（2）系统内置各种网络应用识别协议库和恶意网站 URL 分类库，并能够进行实时更新和个性化选择，提供对恶意网站的过滤，对炒股、游戏、购物、在线视频相关网站的管控功能。

（3）系统可以识别、记录和控制用户对网盘、迅雷、BT 下载、电驴等 P2P 应用，优化网络带宽，保证公司各种业务应用的需求。

（4）系统通过对海量关键词的匹配和过滤技术，实现对 IM 信息交互、BBS 发帖等的合法性管理，帮助企业降低和规避潜在的法律风险。

（5）系统能够实现对用户日常上网行为进行统计和审计功能，使用户的上网行为可视、可控、可查。

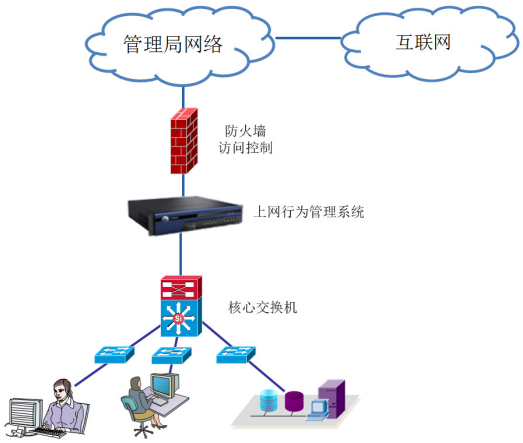
（6）系统为网络管理员提供清晰友好的操作界面，方便网络管理员对网络进行配置和管理。

4.系统建设方案

当前上网行为管理产品主要分为软件方案与硬件网关两类形态。软件方案以 云化部署和轻量级代理为趋势，代表产品包括 Forcepoint、网路岗及域智盾等，支持对终端流量的精细化审计；硬件方案则依托专用设备实现高性能流量处理，国内头部安全厂商如深信服、奇安信、天融信等均已推出整合零信任访问控制与 AI 行为分析的新一代硬件网关，可满足企业级高并发场景下的合规管理需求。

由于相关软件存在兼容性、不稳定、功能不够全面等各种问题，本次系统建设建议使用国内知名信息安全厂商成熟的硬件产品。各信息安全厂商的设备虽然各有特点，但是整体原理和部署方式基本一致。即在公司目前核心交换机和防火墙之间串接上网行为管理设备，对各种互联网流量进行管控。设备采用的是透明串接方式，不影响现有网络架构，并对网络管理员提供方便友好的管理界面。

4.1 系统架构上网行为管理系统的部署结构如下图所示。



根据公司目前的规模和网络状况，兼顾考虑公司未来的发展，本次系统建设按照带宽 10Gbps，用户 2000 人为最低的原则进行选取。

4.2 系统防控功能

上网行为管理系统将解决我公司目前互联网访问缺乏管控措施的问题，提高员工工作效率，保障网络资源合理利用，提高网络可管理性，实现安全、高效、健康的互联网环境。系统功能主要有以下几个方面。

4.2.1 用户管理

用户是上网行为管理产品最为核心的要素，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管理的效果。系统能够根据用户 IP 地址、MAC 地址、域账户、第三方服务器认证等多种方式建立管理用户和用户组，并可以根据需求进行灵活的调整，并基于此建立管理策略，为基于用户或者用户组的策略定制和统计报表奠定基础。

4.2.2 流量管理

系统可限定每个用户所使用的应用类型可占用的带宽资源上下限，管理员可单独控制用户的某项互联网应用（比如 P2P 下载等）可占用的带宽资源上下限，也可以同时控制用户的多项互联网应用可占用的带宽资源上下限。系统可以限制无关应用对带宽的挤占，保障关键业务的使用质量，提升带宽利用率。

4.2.3 网页过滤

Web 是互联网上内容最丰富、访问量最大的应用，然而网页内容良莠不齐，充斥许多反动、暴力、色情以及其它不健康的信息；上网行为管理系统通过预分类过滤技术、URL 自动分类引擎以及灵活的策略设置，对违反国家法律、危害企业安全的内容进行过滤，避免用户有意无意访问包含非法内容的网页，净化网络，减少病毒进入局域网的几率，降低企业法律风险，创造文明健康的上网环境。

4.2.4 应用控制

系统可以限制每个用户允许和阻塞的应用类型，管理员可单独控制用户的某项互联网应用的使用，也可以控制用户的多项互联网应用的使用，甚至可以针对某类应用不同的子应用进行使用控制。如：可限定部分权限用户上班时间允许使用微信、钉钉、QQ 等应用。通过该控制，可以限定公司员工可使用的应用类型的范围，避免无关应用对工作时间的占用。

4.2.5 外发内容审计

为了防止企业机密信息和保密文件外泄，系统将针对 IM、邮件、FTP、论坛发帖等应用的提供全面的审计功能，同时对外发信息进行过滤控制，避免外发不良言论并留存相应记录便于查证，帮助公司规避潜在的法律风险。

4.2.6 统计分析

统计报告是实施上网行为管理设备后进行效果评估的最直观工具，也是了解网络活动以及调整管理策略的最重要的依据。系统能够提供用户/部门网络活动摘要、用户行为统计、带宽资源统计、上网时长统计等各种统计报告，并以文字、表格和图形等多种方式进行呈现给管理人员。

基于对用户上网日志的深度数据挖掘，以指数评估形式直观的向管理者提供员工工作效率分析、网络带宽负载分析，以及员工互联网行为合规分析等分析报告，并对如何提升网络健康指数提出指导和建议。

4.3 系统管理模式

系统可以根据不同的管理级别和管理权限，设置不同的设备管理权限和日志审计权限。企业领导、职能管理部门以及信息管理部门可以根据职能和需求的不同定制不同级别的用户权限，在系统日常运行中发挥不同的作用，保证系统对企业管理制度的高度契合。

5. 小结

在互联网高速发展的时代，建设上网行为管理系统，是实现公司实施网络精细化管理的必然要求。系统的建设应当兼顾流量控制和审计功能，能够实现分级管理，全面满足公司管理制度要求。

目前我公司互联网管理规定和要求相对复杂，对设备策略定制的要求较高。在各厂商设备基本都可以提供设备使用的情况下，建议首先申请设备试用，定制用户和策略后，在生产环境下通过实际的运行不断发现、调整和更正其中不符合管理要求的管理策略，使其最终满足管理要求。在各厂商设备使用完成后，综合考虑其策略符合度、运行效率和设备价格，选择最适合公司的产品，完成系统建设。

[参考文献]

[1][美]斯托林斯 著;白国强，等 译·网络安全基础：应用与标准.清华大学出版社.2004.

[2]深信服科技有限公司. 上网行为管理产品技术白皮书. 深信服官网.2009.

[3]奇安信集团.安全产品.上网行为管理系统.奇安信官网.2025.

[4][美]Saadat Malik 著； 李晓楠 译 . 网络安全原理与实践.人民邮电出版社.2013.