

宝龙汉景网络卫士 信息管理系统 白皮书

版本号：V 6.0

Copyright © 2004 厦门宝龙软件产业发展有限公司. All rights reserved

Address: 厦门市嘉禾路 305 号宝龙中心一期 3F

Tel: (0592) 3979999 Fax: (0592) 5091388

E-mail: linyuz@powerlong.com

URL: <http://www.SoftIBM.com>

目 录

互联网的发展及政府、企业上网中存在的问题.....	3
中国互联网发展的发展概况.....	3
中国专线接入互联网的应用情况分析.....	3
政府、企业专线（含 ADSL 等）接入互联网存在很多亟待解决的管理问题.....	4
政府、企业网络行为管理需求的发展.....	7
宝龙汉景网络卫士信息管理系统功能及优势.....	9
宝龙汉景网络卫士信息管理系统的功能：.....	10
宝龙汉景网络卫士信息管理系统的优势.....	13
为什么选择宝龙汉景网络卫士信息管理系统.....	16
宝龙汉景网络卫士信息管理系统技术介绍.....	18
宝龙汉景网络卫士管理（200 用户标准版）系统功能及参数.....	20

互联网的发展及政府、企业上网中存在的问题

中国互联网发展的发展概况

根据中国互联网络信息中心 2001 年 1 月公布的数据,我国上网计算机数约 892 万台,其中专线上网计算机为 141 万台,拨号上网计算机为 751 万台。我国上网用户人数约 2250 万人,其中专线上网的用户人数约为 364 万,拨号上网的用户人数约为 1543 万,同时使用专线与拨号的用户人数为 343 万。除计算机外同时使用其它设备(移动终端、信息家电等)上网的用户人数为 92 万。

相比 2000 年 1 月的数据,我国上网计算机数为 350 万台,其中专线上网计算机为 41 万台,拨号上网计算机为 309 万台。我国上网用户人数是 890 万,其中专线上网的用户人数约为 109 万,拨号上网的用户人数约为 666 万,同时使用专线与拨号的用户人数为 115 万。除计算机外同时使用其它设备(移动终端、信息家电)上网的用户人数为 20 万。

由此可见,互联网在中国正处于爆破性发展的阶段,互联网已经成为人们生活和工作中的一个组成部分。

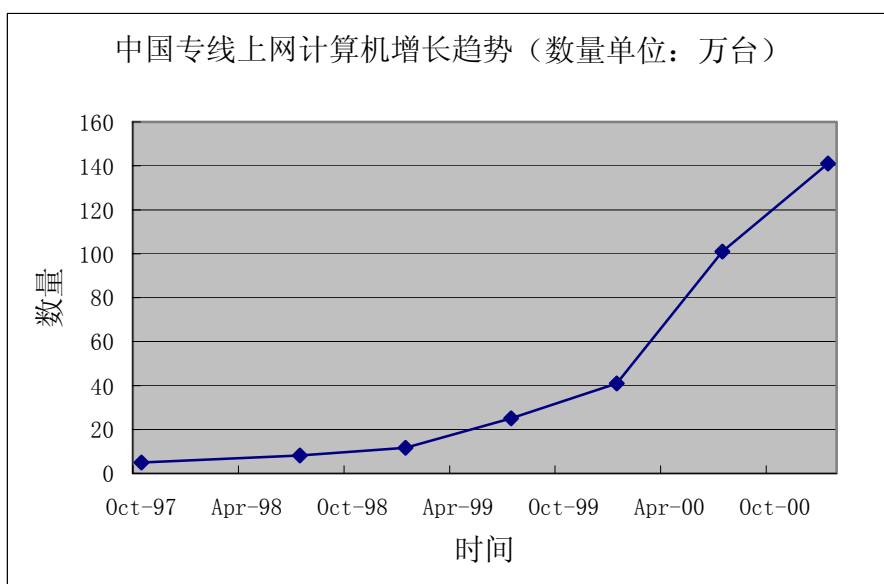
中国专线接入互联网的应用情况分析

下面的数据来自于中国互联网信息中心的历年的调查结果。从专线上网计算机数量上看,增长最快的时期开始于 1999 年初,在 2000 年初又有一次飞跃。如果从年度增长率来看,1999 年到 2000 年,2000 年到 2001 年的增长比例都超过了 300%。另外一个数据同样能说明这个问题,通过专线上网的用户数量 1999 年 1 月仅为 61 万,2000 年 1 月为 224 万,而到了 2001 年 1 月,这个数据已经到了 707 万。年度递增率超过了 300%。

这固然和基础数据低有关,但肯定了专线接入互联网在中国的发展情况,尤其是各类政府、企业已经充分认识到互联网的力量,利用互联网成为各类政府、企业取得竞争优势的一个必不可少的工具。

时 间	专线上网计算机 数量	增长速度
1997 年 10 月	4.9 万台	—
1998 年 7 月	8.2 万台	67%
1999 年 1 月	11.7 万台	43%
1999 年 7 月	25 万台	114%
2000 年 1 月	41 万台	64%
2000 年 7 月	101 万台	146%
2001 年 1 月	141 万台	39%

下图更清楚地显示了专线接入计算机的发展情况：



政府、企业专线（含 ADSL 等）接入互联网存在很多亟待解决的管理问题

毫无疑问，互联网将信息交流提升到一个前所未有的层次，政府、企业经营人员在

获取、收集和发送信息的速度、数量、多媒体的表现形式方面都得到极大的便利，同时相关的成本却降低了。各类政府、企业主或管理人员正是认识到互联网的好处，纷纷开通专线接入互联网，政府、企业内部员工通过局域网就可以方便而快速地享受互联网带来的各种服务。

准确地说，专线接入互联网是政府、企业的一种资源，但目前在利用和管理该资源方面却存在着太多的问题，这些问题极大地困扰着政府、企业高层管理人员、人力资源部和 IT 部门。

■ 网络资源的不合理使用，并导致工作效率下降

根据 IDC 最新数据报导，政府、企业员工平均每天有超过二分之一的上班时间来在线聊天，浏览娱乐、色情、赌博网站，或处理个人事务；员工从互联网下载各种信息，而在那些用于下载信息的时间中，62%用于软件下载，11%的时间用于下载音乐，只有 25%用于下载与写报告和文件相关的资料。

互联网上的内容太丰富了，对政府、企业员工有太多的诱惑，很多的员工沉溺其中，无法自拔，常常把自己的本职工作放在一边，导致政府、企业整体工作效率没有提升反而下降。调查数据显示以下为影响工作效率主要的互联网行为，它们与工作无关而且可能导致更多的问题（比如网络安全等）：

- ◆ 浏览色情网站；
- ◆ 浏览游戏、音乐等娱乐网站，下载大量与工作无关的音乐文件，在线听音乐，在线看视频图像等，不仅耽误工作，而且占用大量的网络带宽资源，影响其他人员使用公司的资源；
- ◆ 浏览相关财经网站，利用公司的资源在线买卖私人股票或浏览相关信息；
- ◆ 浏览“在线”购物和拍卖网站；
- ◆ 浏览赌博网站；
- ◆ 使用即时信息交流软件如 ICQ、OICQ；

.....

■ 网络资源的不公平使用，带来严重的带宽问题

许多上网人员不停地下载大容量的文件，比如大量的 MP3 音乐文件；或者在线听音乐、看视频电影、新闻等行为，严重占用网络带宽，造成网络堵塞，上网速度下降，影响其他员工的正常上网行为。

管理人员奇怪政府、企业大量投资的专线接入速度一天比一天慢；IT 部门经常遭到抱怨，要求提升上网的带宽；而有趣的是抱怨的人中包括那些下载音乐文件或看视频电影的员工。

■ 上网给政府、企业带来的泄密或信息系统破坏等安全问题

任何政府、企业主或管理人员都担心自己内部的机密信息流露出去，而互联网偏偏又方便信息的交流和传递。通过互联网，任何数字文件都可以方便地发送出政府、企业的内部网，正因为如此国外很多公司都对政府、企业内部的电子邮件系统实施定期的检查。但邮件的检查并不全面，因为有很多免费的邮件系统可以利用，它们的使用只要用浏览器就可以；此外即时信息交流软件也可以使用户绕过电子邮件系统而直接发送信息到政府、企业外部。

不受限制的上网行为将带来更多的安全问题，比如下载的文件中带有病毒或其它有破坏性的程序；ICQ、OICQ 等软件的使用有可能招到网络黑客的袭击，硬盘里的资料和数据被窃取或破坏。

想到这些问题，每个管理人员都可能坐立不安。如何解决这些问题呢？

■ 网络资源的非法使用，使政府、企业有可能陷入法律纠纷

在国内，法律规定了很多网站是非法的，比如有色情内容的、与反动政治相关的、与迷信和犯罪相关的等等。使用专线接入互联网后，政府、企业内部网某种程度上成了

一种“公共”上网场所，很多与法律相违背的行为都有可能发生在内部网中。事实上，这是很多政府、企业要加强网络行为管理的最初的原因。

另外一个日渐显露出来的问题是网络黑客利用政府、企业专线入网的条件，实施非法的网络攻击，发送病毒文件等，这都给政府、企业上网带来了许多可能引起法律纠纷的隐患。政府、企业目前缺乏有效的工具在相关事情发生后提供数字化证据。

■ 政府、企业缺乏对网络资源使用进行量化的标准和工具

网络资源作为一种电子化的资源，在是通过政府、企业内部的局域网共享的，网络中的每个登录用户都能使用。专线上网后，到底是哪些人在使用该资源，使用的程度如何，如果要进行相关的成本核算，并把专线接入的成本划到政府、企业内部的每个成本中心，怎样做才是最有效的呢？

互联网或者说信息技术确实是一个“神奇”的东西，在不同的人、不同的组织、不同的政府、企业环境中，它带来的影响是充满矛盾的，能提高政府、企业的工作效率、增加政府、企业的竞争力、降低政府、企业运营成本；另一方面，它却能降低政府、企业的工作效率、给政府、企业带来很多威胁和安全隐患。那么，到底要不要用它？

答案其实很简单，肯定要用，但是必须对它实施有效的管理，就象管理其它的政府、企业资源一样。

政府、企业网络行为管理需求的发展

面对上述如此众多的问题，政府、企业主和管理人员都想到了要对内部员工上网行为的管理。通过对美国和我们国内相关情况的研究，政府、企业这方面的需求从简单到复杂，经历了下面几个阶段。

最初的阶段是严格控制员工的上网，我们称之为互联网接入控制阶段，方式比较简单。政府、企业建立网络地址数据库，规定哪些网站不能访问。几乎大部分网站都被屏蔽，不允许员工在政府、企业网内访问，即使是非工作时间照样禁止。

第二阶段是初步的互联网接入管理阶段，以保持政府、企业的工作效率为目的，通过建立相关的互联网接入策略和管理功能，能实施对不同人员、不同部门的上网权限管理和资源分配，有部分报表系统显示简单的员工访问互联网的记录。

第三个阶段是真正的网络行为管理阶段，以提高政府、企业的工作效率为目的，政府、企业不但建立相关上网策略，更进一步和政府、企业信息系统安全、政府、企业知识管理等结合起来；能更好地分配网络资源，比如对不同对象实现不同的网络带宽分配；建立详细的员工访问互联网的日志，提供详细的报表，能帮助政府、企业管理层分析员工的上网行为，并对上网的策略进行相关调整，让互联网成为政府、企业的最有效的工具。

在上述三个阶段中都有不同的产品相适应，帮助政府、企业实现对专线上网资源的不同层次的管理。就目前的情况而言，各政府、企业在选择产品方面都希望网络行为管理的功能比较强大，能帮助政府、企业管理人员、人力资源部门和 IT 部门解决各自的问题。宝龙汉景网络卫士信息管理系统就是一个很好的工具。

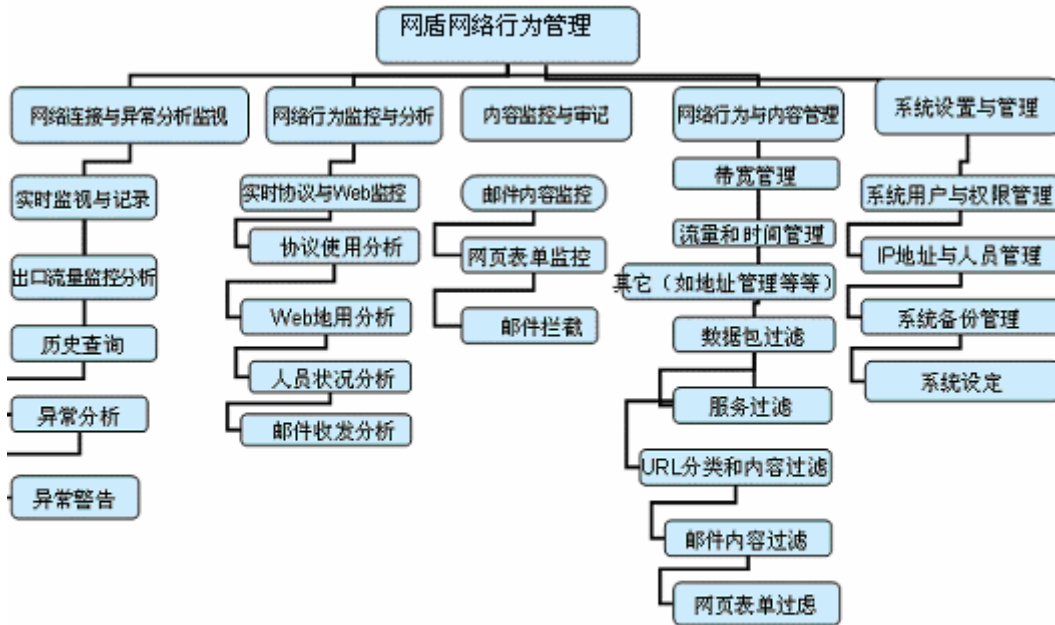
宝龙汉景网络卫士信息管理系统功能及优势

宝龙汉景网络卫士信息管理系统是专为解决各类政府、企业面临的上述问题而产生的产品，通过对市场的详细调查，该系统设计的功能可以满足政府、企业对网络行为管理的第三阶段的要求，帮助政府、企业驾驭互联网接入的宝贵资源，充分发挥互联网的益处，提高政府、企业运营效率，同时降低相关风险。

它是一套对上网用户进行系统管理的纯硬件系统。它不仅能准确记录每个员工所访问的所有网页，而且能对各部门或员工接入互联网的带宽进行分配，提高整个专线接入互联网的效率。

该系统性能稳定、安全性高、功能强大、安装和操作都很方便，是政府、企业对本单位上网管理的理想之选。无论您是想对用户进行上网管理，还是要对用户进行计费管理，拥有了这套系统，这些工作变得十分轻松方便，一切问题迎刃而解。

宝龙汉景网络卫士信息管理系统的功能：



■ 上网权限管理

分配每个员工、每台计算机接入互联网的权限；可以通过组、部门、策略等来形成立体和个性的权限策略。我们的权限支持多级别----个人、部门、系统、策略组、地址段等，我们的权限支持时间段---工作时间、节假日以及自定义的任何时间。通过该功能，政府、企业管理人员可以有效地管理互联网的使用。将互联网资源分配给真正需要的工作人员。避免资源浪费。分配资源的对象可以是具体的员工，也可以是某台计算机或者是某个部门

- 可以按人、组或部门进行互联网访问的控制
- 可以设置允许访问互联网的时间段
- 可以对访问互联网的每日总时间量进行限制
- 可以根据不同的服务协议进行分类控制
- 可以控制用户可以访问的 IP 地址或端口号，限制聊天、流媒体等的应用
- 采用多级用户管理系统

■ 互联网访问管理

限制员工在工作时间访问某些不良或与工作无关的网站，解决员工工作时间玩网络游戏、网上炒股、网上聊天、访问‘黄、赌、毒’等不良网站、工作时间进行购物及其它娱乐活动等行为的管理。防止员工滥用互联网资源，最重要的是提高员工的工作效率。

政府、企业管理人员可以根据需要定制自己的互联网访问策略，增加和删除需要管理的网站地址。

■ 全面细致的审计查询功能

能够审计政府、企业内员工的在线上网行为，记录每个员工所有的上网行为，根据历史记录生成不同的报表，诸如页面访问、收发电子邮件、下载软件、下载文件等；并能妥善有效保存记录，以供管理人员随时查看。

可以查询每一用户或内部网内每一台计算机访问互联网的记录、访问时间、相关数据流量；

可以将相关的数据转化为货币形式，方便对相关部门进行成本核算。

可以查看任一时间内，某个网站的被访问情况，显示究竟是谁访问过该网站以及其所访问过的具体页面；

可以查看某一段时间内部网访问互联网具体的浏览网址列表，方便管理人员分析员工的上网行为，有针对性地作出互联网访问策略的调整。

通过各种报表，管理人员对内部每个员工使用互联网的情况了如指掌，针对上述网络资源管理中的每个问题都能得到数据依据，做相关决策时更准确。

出口流量报告

协议使用报告

协议连接报告

网络流量报告

网络连接报告

端口访问报告

用户使用报告

Web 使用报告

目标连接报告

■ 高效的带宽管理

政府、企业可以根据需要对不同的部门和人员分配网络资源，使他们得到不同的上网速度；不同部门间的上网行为不会互相影响，可以有效地阻止某些人或部门滥用网络资源而影响其他人上网。网盾 ENM 系统可以管理带宽分配的最低单位是字节。

■ 内容监控（邮件、网页表单）

邮件已经成为取代政府、企业原来打印文档和传真文件的一个商业信息传递的重要手段，但政府、企业日益发现，由于没有及时有效的监管，在通过互联网传递的邮件和网页表单中也存在着很大的信息安全隐患，如何对信息进行有效的监管和控制，对可疑的部分进行审核。适应政府、企业的这种需要，宝龙汉景网络卫士信息管理系统率先开发出内容（邮件、网页表单）的审计功能。

■ 中文网址库模块

自动在线升级，多大 40 多个分类，近百万的中文专业分类，分类涉及政府、企业管理头痛的色情、暴力、反动、娱乐、交友、视频、游戏等等。目前是国内唯一针对中国人上网特点定制的权威数据库。

■ 网络计费模块

针对校园、宾馆、政府、企业等上网计费的需求，宝龙汉景网络卫士管理计费模块可以完成按流量、时间、分时段、包月、预付费等多种灵活的计费方式，灵活易于管理。同时支持 IC 卡接口。

■ 开放接口模块

网盾是一个基于协议的开放平台，它同时提供了和其他网络安全、网络管理和数据库应用的大量接口。这些接口包括邮件审计远程备份接口、上网记录的数据库接口、防火墙接口、入侵检测接口、代理服务器（Proxy）接口、Cache Server 接口等等。

■ Cache 代理模块

系统内置稳定的、高效的 cache 代理模块。支持 http 和 ftp 缓存。

宝龙汉景网络卫士信息管理系统的优势

宝龙汉景网络卫士信息管理系统除了上述全面的功能外，还具有如下优势：

■ 各自独立的功能模块

上述各大功能均有相应独立的功能模块，用户可根据自己的需要进行组合。

■ 安全稳定

保证了系统运行的高效性；系统可以以旁路或网桥方式（视客户具体网络结构而定）连接在网络中，系统硬件符合 Intel 服务器平台标准。

■ 安装简单，即插即用

本系统是一套独立的纯硬件系统，无需专用的管理程序和管理平台；对用户的操作系统平台无特别要求；用户可完全保留现有的网络结构和配置，使用该设备时只需要接在内部网，开机后经过简单的设置即可使用。

■ 性能卓越

采用先进的架构及算法，在百兆的网络上，系统的最大带宽可达到 86M，若网络的带宽小于 86M，系统对网络的带宽没有影响。

■ 加密操作

本系统采用 SSL 认证等数据加密传输技术以保护网络通讯的安全。

■ 操作方便快捷

本系统全部采用 WEB 管理界面，无论管理人员还是普通用户，都能方便使用。管理人员还能对该系统实施远程管理控制。

■ 标准化设计

包分析和过滤器设计完全按照 RFC 的相关标准。支持的 RFC 标准有：

RFC 821 - Simple Mail Transfer Protocol

RFC 1652 - SMTP Service Extension for 8bit-MIMEtransport

RFC 1842 - ASCII Printable Characters-Based Chinese Character
Encoding for Internet Messages

RFC 1869 - SMTP Service Extensions

RFC 1892 - The Multipart/Report Content Type for the Reporting of
Mail System Administrative Messages

RFC 1893 - Enhanced Mail System Status Codes

RFC 1894 - An Extensible Message Format for Delivery Status
Notifications

RFC 1939 - Post Office Protocol - Version 3

RFC 1957 - Some Observations on Implementations of the Post Office
Protocol (POP3)

RFC 2449 - POP3 Extension Mechanism

RFC 3046 - DHCP Relay Agent Information Option

RFC 3027 - Protocol Complications with the IP Network Address Translator

RFC 3022 - Traditional IP Network Address Translator (Traditional NAT)

RFC 2990 - Next Steps for the IP QoS Architecture

RFC 2965 - HTTP State Management Mechanism

RFC 2964 - Use of HTTP State Management

RFC 2936 - HTTP MIME Type Handler Detection

RFC 2878 - PPP Bridging Control Protocol (BCP)

RFC 2101 - IPv4 Address Behaviour Today

RFC 2100 - The Naming of Hosts

■ 开放性接口

数据库接口：通过宝龙汉景网络卫士信息管理系统，可以将记录的数据导出到各种数据库进行进一步数据挖掘。

邮件远程备份接口：通过网盾提供的 POP3 接口，导入到远端服务器的 OE（Outlook Express）内，进一步备份和方便查询。

为什么选择宝龙汉景网络卫士信息管理系统

宝龙汉景网络卫士信息管理系统最重要的是能够帮助政府、企业管理好互联网资源，管理好员工的上网行为，使政府、企业真正利用互联网这个强大的工具来提高生产力，增加政府、企业的盈利能力。

宝龙汉景网络卫士信息管理系统采用经过 **inter** 认证的硬件和专有的嵌容式操作系统，以保证整个系统的安全、稳定和高效。

宝龙汉景网络卫士信息管理系统分配合理的权限给合适的工作人员，内容过滤功能可以限制政府、企业员工访问非法站点和与工作无关的站点，审计查询功能帮助政府、企业跟踪员工的上网行为，对一些不良、违法行为起到威慑作用，并能够帮助政府、企业提取数字证据。

宝龙汉景网络卫士信息管理系统有功能强大的计费系统，能帮助政府、企业管理人员掌握每个员工的上网时间、上网的数据流量，同时能进行精确的成本核算。

宝龙汉景网络卫士信息管理系统的带宽管理模块，能帮助网管人员、管理人员分配好有限的网络资源，对重要的用户和普通用户分别设置其上行带宽和下行带宽，防止因个别用户因下载大容量文件，造成网络阻塞，使其他用户的正常上网行为受影响。

宝龙汉景网络卫士信息管理系统，为政府、企业用户提供了最简单的接入方式，即可完成所需的功能，不改变原有的网络拓扑结构和相关的配置。最大限度地方便政府、企业网络管理者的管理。宝龙汉景网络卫士信息管理系统是独立的硬件系统，其安装与政府、企业用户原有的网络无关，运行稳定，性能出众。

宝龙汉景网络卫士信息管理系统充分为客户考虑，模块化的系统结构帮助政府、企业

用户量身定做自己的网络行为管理系统，客户可以根据自己的需要进行灵活的组合。

宝龙汉景网络卫士信息管理系统提供数据备份和恢复的功能，政府、企业用户可定期备份 HTTP 记录或用户数据。在系统出现意外情况，数据被破坏时，进行数据恢复。

宝龙汉景网络卫士信息管理系统技术介绍

宝龙汉景网络卫士信息管理系统，是一个对政府、企业内部网与互联网之间传输的数据进行监控管理的硬件系统。该系统采用了先进的架构和技术，不同于传统的基于代理的互联网接入控制系统的工作方式，克服了其无法克服的技术瓶颈，从功能、性能、效率、安全性等方面全面超越传统的互联网接入控制系统。

宝龙汉景网络卫士信息管理系统集中了多项先进实用技术，如系统的多种工作方式、基于帐号的审计方式、包过滤、基于状态的内容检测、带宽管理、通信加密等。

系统的接入方式

宝龙汉景网络卫士信息管理系统以旁路、网桥和 NAT 的方式连接在内部网的出口上。网络上流入、流出的数据包通过该系统，系统可以根据用户需要对具有某种特征、状态的数据进行记录，处理，有效实现对网络数据的监控。

其中网桥方式的连接，具有以下几个优点：

- 不占用 IP 地址：不仅节约了网络资源，还避免了对网络上现有设备配置的改动。
- 不改变现有的网络拓扑结构：该系统对用户的网络结构无特殊要求，使用该系统不会对用户现有的网络拓扑结构造成影响。
- 效率高：与基于路由的工作方式相比，不仅避免了繁琐的路由表的维护，还提高了数据传输的效率。
- 透明：系统的内外两个接口没有 IP 地址，对内、对外都是透明的。
- 安全：没有 IP 地址和端口，有效防止了网络黑客对系统的攻击行为。

对于大型政府、企业，由于系统的稳定性要求极高，我们建议采用旁路的接入方式进行。

基于帐号的审计方式

宝龙汉景网络卫士信息管理系统不仅支持基于 IP 地址的审计方式，还支持基于用户帐号的审计方式。对于内部使用动态分配 IP 地址的政府、企业，或高校内的公共机房等场所，基于 IP 地址的审计方式无法真实准确的将网络行为管理实施到每个网络用户，而基于帐号的审计方式就可以满足需求，这使得该系统管理的对象可以是政府、企业的员工，也可以是某台计算机。它主要有以下特点：

- 防止 IP 地址盗用造成的网络行为管理问题。
- 解决了动态分配 IP 地址的网络行为管理问题。
- 解决了同一 IP 地址被多人轮流使用的网络行为管理问题。
- 可实现对用户邮件使用进行管理。

包过滤

宝龙汉景网络卫士信息管理系统是安装在内部网络的出口位置，对网络上流入、流出的数据包进行过滤，允许正常的数据包通过，拒绝非法或异常的数据包通过，具有以下几个功能特点：

- 禁止非授权用户访问互联网的企图。
- 防止来外部对内部网络状况探测的企图。
- 禁止外部访问内部的重要计算机
- 实现包过滤防火墙的基本功能

基于状态的内容检测

宝龙汉景网络卫士信息管理系统采用基于状态的内容检测技术，对内部网上网用户访问的站点、页面进行监控，根据站点的 IP 地址、域名、关键字进行监控，禁止上网用户访问

某些站点，记录上网用户访问过的站点、页面，为管理员提供必要的电子记录。

带宽管理

对内部用户占用的网络带宽进行适当的分配管理，根据用户的 IP 地址，限制某个时间段内用户发送或接收的数据包的数目，达到对内部上网用户实际使用带宽的限制，防止了个别用户恶意占用带宽而造成对其它用户上网的影响。

宝龙汉景网络卫士管理（200 用户标准版）系统功能及参数

特性	说明
最大带宽	80M
平均无故障运行时间	15000 小时
最大连接数	60000
支持的应用协议	基于 TCP/IP UDP 的上网行为
支持的用户帐号数	2000
数据保存的时间	500 万条上网记录和 80G 存储空间

*以上参数仅供参考，具体受软硬件环境影响，数据会有所不同。