

网络特警™ 白皮书

LinkQos Introduction

——专注多网段、大规模网络环境上网行为管理！

——专业限制 P2P 下载、聊天、炒股、游戏、带宽流量！

大势至（北京）软件工程有限公司

2011 年 8 月

网络特警™ 产品简介

目录

网络特警™背景简介.....	3
网络特警™核心理念.....	6
网络特警™核心优势.....	9
网络特警™独特架构.....	15
网络特警™功能列表.....	31
网络特警™服务体系.....	41
联系我们.....	42

网络特警™上网行为管理系统的研发背景和总体概述

当前随着企业信息化和电子政务工程的推广，国内各行业企事业单位都创建了自己的内部局域网，应用了各种信息化系统来提升生产和工作效率，网络规模也日渐扩大，网络管理面临的诸多问题也逐步暴露出来，网络管理和网络监控面临着新的挑战。

长期以来，国内网管软件市场以纯软件架构存在，网管软件产品以其门槛和技术含量较低，投入少、更容易推广等特征而在市场上泛滥，造成国内网管软件质量层次不齐，厂商大小不一，产品同质化严重，网管软件市场呈粗放发展状态。

网管软件市场的不规范、不健康、粗放式发展也影响了用户的选择，加之网络管理、网络监控是一个新生的管理理念，一些厂商出于市场利益和产品宣传的需要而向用户灌输一些错误的概念、思想、术语等，误导了用户的选择，使得用户一方面无法实现相应的网络管理，另一方面也造成了投资的浪费。这些行为使得用户对网络管理软件建立了不好的印象，严重影响了网管软件市场的健康、良性发展。

作为国内最早的专业上网行为管理软件，多年来聚生网管系统以部署最快捷、功能最实用、使用最简单、性价比最高等各项领先优势在国内同类网管软件中遥遥领先，极大地推动了国内各行业企事业单位的网络管理水平，为国内网管软件市场的健康发展做出了较大贡献。但是，随着企事业单位网络规模的不断扩大，网络管理问题的逐步增多，用户对网管系统的稳定性、高可靠性、高性能需求的不断强烈以及聚生网管产品自身定位等原因，使得研发基于硬件嵌入式架构的网管系统的研发已经是大势所趋。

大势至（北京）软件工程有限公司以推动行业健康发展为己任，紧跟行业发展新趋势，深刻领悟广大用户的核心需求，经过近三年的研究和技术储备，终于在 2010 年 6 月实施了网络特警™硬件网管产品的开发，于 2011 年 6 月最终开发完成。

网络特警™上网行为管理系统是大势至（北京）软件工程有限公司汇聚六年网络管理技术和实践经验的一次集中提炼和升华，是在全面总结现有硬件架构的网管系统的诸多不足，在深入调查用户网络管理的真切需要的前提下并凝聚大势至全体人员不畏困难、大胆突破、

不断创新和反复实验的基础上研发成功的一款全新的基于硬件嵌入式芯片的上网行为管理产品。



网络特警™外观（1U/2U 架构）

平台架构	标准 1U/2U 工业设计，高强度钢外壳
CPU	支持 Intel Core i3/i5/i7
内存	4G-16G, DDR3/1333MHZ
硬盘	500G-2TB 高速 SATA 硬盘
网卡	Intel PCI-E 高性能千兆/万兆网卡
LAN BYPASS	2 组
峰值流量	10G
工作温度	0-60°

网络特警平台参数

网络特警™基于“创新直连”架构，可以直接连接局域网二层交换机、三层交换机、核心交换机等设备即可实现对局域网所有电脑的上网行为的全面控制，不需要在交换机做端口镜像、不需要部署 HUB 集线器、不需要安装代理服务器等，也无需将网络特警™“串接”、“桥接”、“旁路”在交换机和出口网关（路由器、防火墙）之间，从而极大地简化了部署网管系统的复杂性、工作量和风险，也极大地降低了网络数据包的延迟，避免了部署网管设备对网络性能的消耗。

网络特警™具有聚生网管系统的全部功能和优势，并且以“创新直连”架构、“跨网段 IP 和 MAC 绑定、多重网络管理防护、同级别性能最高等独具特色、极具竞争力的多项领先优势，成为引领当前国内硬件监控系统的标杆产品，是大势至（北京）软件工程有限公司推出的面向大中型企事业单位的高端网络管理系统。

总之，网络特警™上网行为管理系统以功能最实用、使用最简单、部署最快捷、服务最实时、性价比最高等诸多优势成为国内各行业企事业单位加强上网行为管理、提高网络资源利用效率、提升员工工作效率并最终为企事业创造良好的网络管理收益和经济效益的不容置疑的选择！

网络特警™上网行为管理系统核心理念

网络特警™上网行为管理系统是大势至（北京）软件工程有限公司在充分分析当前网络管理系统的诸多不足，充分吸收当前网络管理的最新技术，以及聚生网管系统多年积累的网络管理经验基础上，并且以彻底解决当前国内各行业企事业单位面临的诸多网络管理问题为最终目标而推出的一款硬件嵌入式架构的网络管理系统。其核心思想主要有以下几个方面：

一、 严肃网络管理，提升网络资源利用效率，创造网络管理收益和经济效益。

当前国内很多企事业单位的各项业务越来越依赖于各种信息化系统，踏上网络之路、提高工作、生产效率已经成为当前企事业单位的普遍共识。为此，很多企事业单位不惜花费重金购买更高速率的宽带服务。但是通过实际调查我们得知，很多企事业单位的网络资源常常捉襟见肘，上网速度慢、信息传递延迟、信息化系统不能正常工作、无法开视频会议，甚至打开网页、收发电子邮件都十分困难。究其原因，很多情况下不是单位的网络带宽速率不够，而是这些宝贵的网络资源正在被与工作无关的各种互联网应用给耗尽了。分析起来，不外乎是 P2P、BT 下载；在线视频；股票软件；网络游戏等等。因此，有效控制员工上网行为，杜绝不合理的网络应用，提升企事业单位网络资源利用效率，保证网络的安全、稳定和畅通，使得企事业单位的网络资源真正为企事业单位创造经济效益和社会效益，就成为当前企事业单位网络管理的核心诉求，而这也是网络特警™上网行为管理系统的研发的初衷和终极目标。

二、 提供更稳定、更可靠、更高性能的网络管理系统

网络特警™上网行为管理系统是依据“高内聚、低耦合”的软件核心研发原则，并通过对聚生网管系统核心代码的全部重构基础上推出的全新版本，较之于聚生网管其核心代码量降低 30%，编译成功后软件形态仅 2 兆大小，是国内体积最小的专业网络管理系统，从而大大避免了庞大冗繁的代码普遍存在的系统不稳定问题，使得系统的稳定性、健壮性和可靠性大幅增加；同时，借助于自主研发的高性能工业计算机，能够适应严酷的运行环境，稳定运行 10 万小时无宕机，集成的 Bypass 功能可以确保网络异常时的零延迟网络恢复功能；同时大势至公司研发团队通过对网络特警™所依赖的操作系统进行进一步的优化和提升，使得比

同类、同配置的网管设备至少提升 30%的综合性能。总之，高质量的软件代码和高性能、高可靠性的硬件架构，为网络特警™上网行为管理系统的稳健运行提供了前提、基础和保障。

三、 网络管理的实时、个性化、按需定制服务

网络特警™上网行为管理系统有别于其他硬件架构网管系统对客户个性化需求置之不理，或者定制个性化功能（比如封堵一款新出现的 P2P 软件、聊天软件、股票软件、网络游戏）或者其他合理的网络管理需求需要付出高昂的费用，或者需要较长的研发周期等。网络特警™上网行为管理系统针对用户的个性化、合理需求实行实时、个性化定制服务（比如最快 2 分钟即可封堵一款最新的股票软件、网络游戏或者聊天软件），从而可以充分满足客户个性化的网络管理需要——我们开发的诸多网络管理插件（如代理扫描器、外来电脑隔离器、主机异常警报工具等）既是针对客户个性化需求而开发的，这些定制服务根据实际情况酌情收取一定费用或者完全免费，从而一方面满足了用户的个性化需要，另一方面也使得客户得到网络管理的最大实惠。

四、 部署最快捷、使用最简单、功能最实用的思想

网络特警™上网行为管理系统的诞生和聚生网管系统有诸多类似之处。首先，基于“创新直连”架构的网络特警™上网行为管理系统依旧是国内硬件监控系统里面部署最快捷的、最省心、工作量最小的。与其他硬件监控系统采用串接（采用双网卡，一块接内网交换机，另一块接出口网关路由器等）、旁路（采用端口镜像、部署 HUB 集线器或代理服务器）不同，网络特警™上网行为管理系统只需要连接内网交换机即可（无论是基于二层、傻瓜交换机的单网段环境还是基于三层、核心交换机的多网段环境），从而可以实现最快捷、最省心、工作量最小、对网络没有任何调整的部署。其次，网络特警™上网行为管理系统界面和使用方式完全继承聚生网管系统，所有的网络管理功能点点鼠标就可以完全实现，是当前国内使用最简单的网管系统。不仅如此，网络特警™上网行为管理系统的所有相关组件都在出厂之前安装配置完毕，客户只需要点点鼠标启用即可，甚至还可以建立一键还原，从而保证系统可以永续运行；最后，网络特警™上网行为管理系统核心网络管理功能继续保持领先，尤其是在完全禁止迅雷下载、禁止 Skype 聊天、限制上网带宽、控制网络游戏、封堵股票软件等诸多方面。

五、 提供整体的网络管理解决方案而非单纯一款硬件监控系统

网络特警™上网行为管理系统不仅是提供给用户一套硬件网络监控系统，更是一种网络管理解决方案。大势至（北京）软件工程有限公司凭借在网管软件、网络管理领域长达 8 年的研发、实践经验，积累了大量的网络管理方法、技术和文档，从而可以在硬件监控系统之外提供一套软性的网络管理方案，这些资料涉及到网络管理、网络监控的方方面面，可以帮助网管人员迅速提升网络管理技术，从而在更高水平上提升网络管理，帮助企业提升总体的企业管理水平。大势至公司明白，单靠一套监控系统，无论其功能如何强大，也无法能够保证最大的网络管理效果。为此，我们在国内首创“软硬结合”的网络管理思想，引领了网络管理的大方向。

六、 硬件按照用户网络环境按需定制，维修服务本地化思想、提供最大便利

网管设备出现问题或者因老化需要升级怎么办，这是所有硬件监控系统都面临的潜在问题。通用的做法是：由用户将网管设备邮寄给网管系统厂家，由厂家提供维修、升级和维护。但是，由于往返周期较长，费用较高，风险较大，网络管理中断时间长等特点，使得用户对这种方式颇有微词。我们认为，所有以客户为中心的网管系统厂家，都应该以最方便客户、对客户利益最大化为基本的商业原则。为此，我们与其他网管系统厂商不同，在提供给用户的硬件监控设备在出厂之前可以为用户进行无偿免费升级，不仅满足用户当前的需要，更能满足用户长远的硬件性能需求，防止网管系统因设备陈旧过时而导致网络管理性能下降、网络监控效率因网络规模扩大而无法负荷或者降低的情况发生，这也使得网络特警™上网行为管理系统的硬件载体是国内同类网络管理设备中性能最强、扩展性最强、性价比最高的网管设备；同时，一旦监控设备在保修期出现问题，我们建议用户在本本地就近维修，而后只需要向大势至公司提供相关的维修发票，即可为用户全额报销，从而可以尽可能降低用户的维修周期，最大程度上便利了用户的网络管理。

网络特警™上网行为管理系统十二大核心优势

网络特警™上网行为管理系统是大势至（北京）软件工程有限公司在充分总结聚生网管系统多年的技术、实践和网络管理的经验，充分倾听用户网络管理需求，深入研究国内同行业网络管理厂家产品的缺陷和不足，适时吸收当前最新的网络管理技术的基础上研发成功的一款基于硬件嵌入式芯片的专业网络管理系统。网络特警™上网行为管理系统以诸多核心优势，遥遥领先国内同架构、同级别网络管理系统。其主要核心优势如下：

网络特警™上网行为管理系统遥遥领先国内同类网管系统十大核心优势：

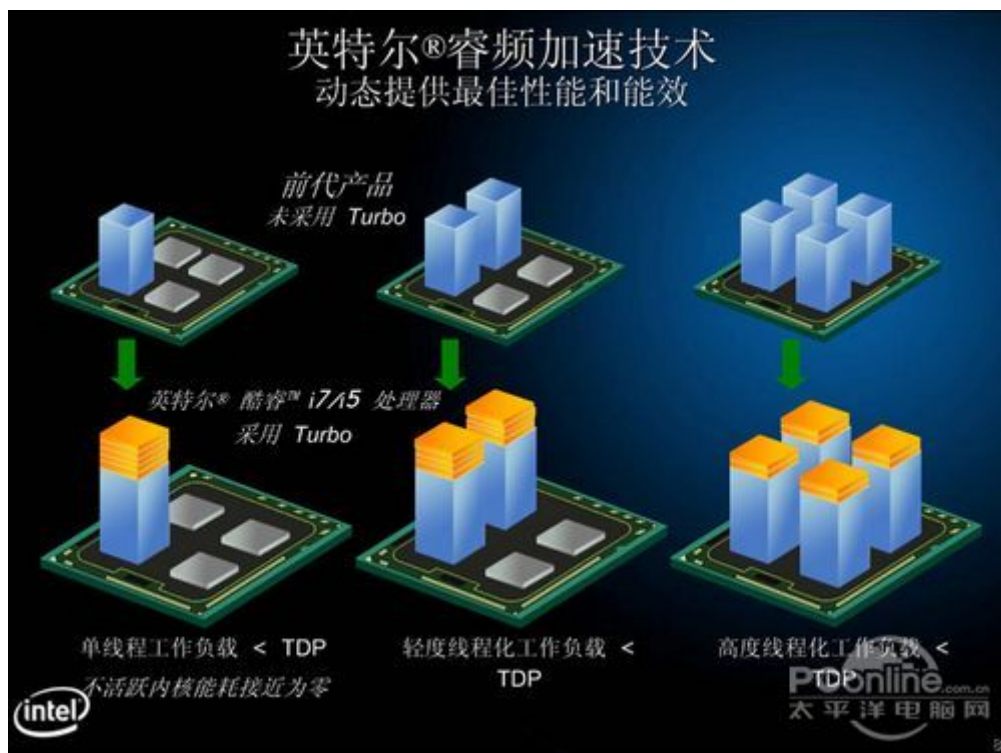
一、不调整现有的任何网络结构或添加额外网络设备，热插拔式、全透明部署，一台设备管理整个局域网的上网行为

网络特警™上网行为管理系统的首要优势：不需要安装客户端软件、不需要调整网络结构或者增减网络设备，不需要在交换机做端口镜像、不需要代理服务器或者部署 HUB 等网络结构，也不需要双网卡串接、桥接到交换机和出口网关（路由器、防火墙等）之间等方式来部署。网络特警™基于“创新直连”架构，而只需要将本设备接入交换机（二层交换机或三层交换机）就可以控制整个局域网的任意主机的 P2P 下载、任意聊天软件、任意股票软件、任意网络游戏、网页浏览、限制主机的带宽流量、进行 IP 和 MAC 绑定以及隔离危险主机等一切网络行为；同时，和国内其他网管系统采用 ARP 技术不同，网络特警™基于 IP 协议、ICMP 包重定向技术，从而可以完全避免因为一些防火墙而导致网管系统、网络管理功能受到影响的情况。相反，在客户部署网络特警™的情况下，我们鼓励客户在客户端电脑上安装各种防火墙，以保证内网安全！

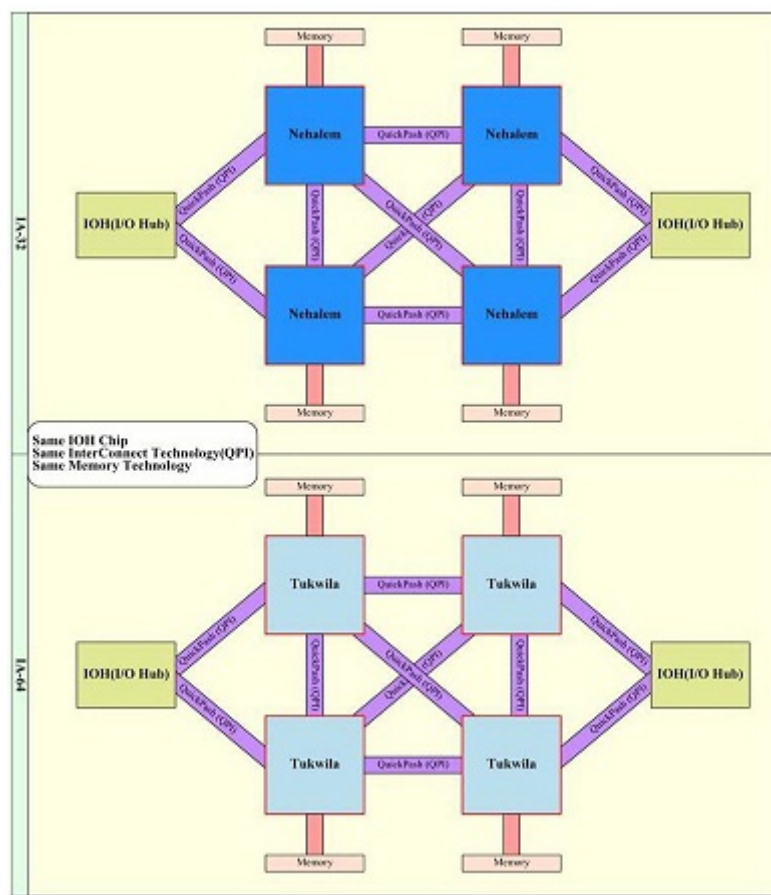
二、基本硬件配置比同类网络管理系统、同配置硬件平台至少提升 40%的综合性能

网络特警™上网行为管理系统所依赖的硬件平台是国内首家公开内部具体配置（CPU、主板、内存、网卡、硬盘等）的监控系统。国内同类硬件平台的互联网行为网关、上网行为监控设备一般对具体的硬件配置讳莫如深，一般不会公开其相关配置。这是因为很多网管设备厂家所采用的硬件配置，尤其是 CPU 常常采用 Atom、赛扬、奔腾 D 等上网本或者低端电脑

所采用的 CPU，而内存一般也是采用容量小的一代（DDR333 或 DDR400）内存，网卡一般采用普通 PCI 网卡（共享总线、性能低）。这些配置连用户当前的普通 PC、台式机的配置都不如，因而性能较低、网络延迟大、甚至在较大网络流量下会出现死机现象，导致用户局域网发生网络中断，影响正常上网。大势至公司推出的网络特警™硬件平台一改行业之先河，不但对用户公开具体的硬件配置，甚至还对全新产品规定了最低配置（CPU 为酷睿 2 双核、内存 4G、硬盘 500G），从而可以提供更高的网络监控效率；不仅如此，网络特警™内置基于英特尔 PCI-E 技术（独享总线，比普通千兆网卡性能提升 10 倍！）的数据转发专用网卡，从而进一步提升了网管系统的抓包性能；在中高端网络特警™型号里面我们采用英特尔最新的 i5 系列 CPU，通过增强的睿频技术（Turbo Boost）和快速通道互联技术（QPI）可以大幅度提升数据包处理效率，如下图所示：



英特尔睿频加速技术（Turbo Boost）技术架构图



英特尔快速通道互联技术（QPI）

三、独家对监控设备所预装的操作系统进行全方位的优化，至少提升 30%的系统性能

很少有上网行为管理系统提供商或者用户注意操作系统对网管系统的影响，实质上操作系统本身承载了很多不必要的应用和限制，这极大地拖累了操作系统综合性能的发挥，进而影响到网管软件自身的运转性能。为此，大势至研发团队通过对硬件预装的操作系统全面优化和提升，使得网络特警™可以在操作系统层面至少再提升 30%的综合性能，从而使得网络特警™上网行为监控系统成为当前国内同类网管系统、同类硬件平台下、同操作系统平台下性能最高的网管设备！

四、网络特警™上网行为管理系统是国内唯一可以完全封堵迅雷(迅雷 5 或者 Web 迅雷)的网管系统

和聚生网管一样，网络特警™是国内唯一可以完全封堵迅雷上传和下载的网管设备。此外网络特警™上网行为管理系统可以有效封堵的 P2P 下载工具和 P2P 视频工具有：

BitComet(比特彗星), eMule(电骡), eDonkey(电驴), Poco/PP 点点通, Kamun(卡盟), 迅雷多点, Vagaa(哇嘎画时代), Kugoo(酷狗), Baidu 下吧, BitSprit(比特精灵), μ Torrent, 百宝, Shareaza(Raza), aBitCool(网酷), Tuotuo(脱兔) PPLive, PPFilm(皮皮影视), PPVOD(PP 点播), PPStream(PPS 网络电视), QQLive(QQ 直播), ViviPlay(TVKoo 网络电视), UUSee(悠视网网络电视), CoolStreaming, 沸点网络电视, PPMate(网络电视), 猫眼宽频, TVAnts(电视蚂蚁)等等, 是目前国内限制 P2P 软件最多、最有效、最彻底的网管系统。

五、国内唯一可以完全封堵号称“网管杀手”的 SKYPE 等网络电话软件, 甚至在国外也遥遥领先

近几年, TOM 公司推出的 Skype 是全球最清晰的网络电话, 具备 IM 所需的其它功能, 比如视频聊天、多人语音会议、多人聊天、传送文件、文字聊天、网络电话等功能。由于 Skype 通过 P2P 方式登陆, 也就是说它可以自动在全世界范围内搜索用于登陆的服务器, 可以支持从 443、80 端口进行登陆, 所以已经无法通过封堵 IP 和端口的方式来封堵 Skype 了, 而与此同时, Skype 的传输协议进行了加密, 从而也无法识别其传输特征, 从而使得 Skype 成为当前最难封堵的聊天工具软件, 成为了名副其实的“网管杀手”! 而网络特警™上网行为管理系统通过集应用网络协议最新的智能解析技术, 并通过长期的研究总结, 终于实现了对 SKYPE 的完全封堵, 从而为国内外网络管理人员解决了燃眉之急, 成为国内网管人员不容置疑的选择!

六、点点鼠标即可封堵腾讯 QQ 高达 12 种国内最流行的聊天软件, 不需要额外添加 QQ 服务器 IP、端口等

网络特警™上网行为管理系统可以完全封堵的聊天工具有: QQ, MSN, 网易泡泡, 新浪 UC, QQ 传文件, MSN 传文件, AIM(ICQ), Skype 网络电话, SoQ 搜 Q, 阿里旺旺, 雅虎通 Yahoo, IRC 等等, 同样也是国内限制聊天工具最多、最有效的网管系统。特别是网络特警™上网行为管理系统控制 QQ 只需要点点鼠标就可以完全封掉, 而国内类似网管系统需要在路由器、防火墙添加大量的 QQ 服务器 IP 来实现, 操作复杂, 也常常无法对聊天软件做出有效的封堵。

七、点点鼠标即可封堵国内流行的 20 多种股票软件, 目前国内封堵最多、最简单、最有效

网络特警™上网行为管理系统可以有效封堵的炒股软件有：大智慧(包括大智慧新一代)、同花顺、广发至强版、龙卷风行情分析软件、钱龙旗舰、国元证券软件、分析家、麒麟短信王、光大证券超强版、证券之星、国信证券、申银万国等等。同时，我们可以随时为客户增加新出现的股票软件，最快 10 分钟即可增加一款股票软件的封堵规则。

八、点点鼠标即可封堵当前国内流行的 30 余种网络游戏，目前国内封堵最多、最简单、最有效

网络特警™上网行为管理系统目前可以有效封堵的网络游戏有：QQ 游戏、QQ 农场游戏、开心网游戏、开心农场游戏、泡泡堂、QQ 游戏、边锋游戏、浩方游戏、POPO 游戏、中国游戏中心、同程游戏、youxi518 游戏、youxi8848 游戏、38game 等游戏、联众游戏、上海热线，并且集成了当前国内所有流行的网络游戏网址列表，可以轻松封堵在线游戏、网页游戏。同时，我们可以随时根据用户的需要增加新出现的网络游戏的封堵规则，最快 10 分钟即可为客户定制一款新出现的网络游戏的封堵规则。

九、可以实时、精确、直观地控制局域网任意主机的流速(带宽)，也即上网带宽、上网速度，而不仅仅只是控制流量。

网络特警™上网行为管理系统可以实时查看、精确控制局域网任意主机的带宽(流速)和流量，而国内其他网管系统由于需要在交换机做端口镜像、部署代理服务器或者 HUB 等方式，所以一般只能限制流量，无法对局域网各个主机的带宽(流速)占用情况进行有效的控制，从而也无法真正实现对网络资源合理分配的目的。

十、可以完全隔离外来电脑、隔离局域网中病毒电脑或者危险电脑，有效防止蠕虫、冲击波和黑客的入侵。

网络特警™上网行为管理系统独创的局域网主机强制隔离技术，不需要客户端就可以对外来电脑、局域网中病毒的电脑或者非法接入网络的电脑进行完全的隔离，被隔离的电脑将中断同局域网其他主机的连接，无法访问局域网其他电脑的共享资源，同时也无法访问公网，从而阻止了病毒在局域网的肆虐，保护了企业的网络安全和信息安全。

十一、有效检测处于混杂模式的网卡，从而可以精确定位黑客软件、Sniffer、wireshark等嗅探软件和其他网管软件

可以有效检测局域网内网卡处于混杂模式的电脑，从而可以帮助网管人员发现局域网电脑可能运行 Sniffer 嗅探软件、网管系统、黑客软件等危害局域网安全的工具软件，从而保护了网络安全。（国内首推、国内首家！）

十二、可以有效检测局域网内代理服务器和代理软件，禁止电脑通过代理上网或充当代理服务器

可以检测局域网代理服务器，帮助网管人员精确扫描局域网 HTTP 代理和 SOCKS 代理，从而可以帮助网管人员禁止局域网电脑通过代理服务器上网、通过代理软件上网，并禁止局域网电脑充当代理服务器，从而极大地保护了内网安全，也强化了网络管理。（国内首推、国内首家！）

网络特警™上网行为管理系统系统的十大核心优势，正是针对当前网络管理的种种难题而创设的有效解决方案，从而也无可争议地成为国内网管系统选型的标准，也成为衡量网络管理是否达标的关键指标。网络特警™上网行为管理系统公司也会不断强化各项领先优势，势将中国网络管理水平提升到新的境界，不断为各行业创造良好的管理效益和社会效益！

网络特警™ 上网行为管理系统独具特色的领先架构

网络特警上网行为管理系统采用基于“创新直连”架构的部署方式，与国内主流网管系统完全不同，具有明显的领先优势。“创新直连”这一概念由大势至（北京）软件工程有限公司首先在网管软件领域提出。顾名思义，就是将上网行为管理系统（或设备）直接（同时也只需要）连接交换机或者路由器等网络设备即可实现对交换机下面所有电脑的上网行为的全面监控，不需要对现有的网络结构做出任何调整，也不需要添加额外的硬件设备。同时，如果在某些情况下需要停止本监控设备的运转，则可以将本设备直接移除网络即可自动导通，对网络没有任何影响，对局域网来说是全透明部署。

当前国内主流的网管系统一般是通过旁路、串接（网关）的等四种方式来部署。旁路的方式一般是需要在交换机做端口镜像、部署 HUB 集线器或者代理服务器的方式；而串接和桥接的部署方式，一般是通过在监控设备里面部署至少两块网卡，一块网卡连接三层交换机，另外一块网卡连接出口网关（路由器、防火墙），然后将这两块网卡桥接起来，然后将内置的监控软件部署在此虚拟的“网络桥”上对过往的报文进行识别、过滤和拦截，以此实现对电脑上网行为的管理。公平地说，上述几种部署方式都有自己的优缺点，我们下面有图示一一加以说明。

一、第一代网管系统：旁路方式部署（早期纯软件架构的网管系统多用此种方式部署，分为端口镜像、Hub、代理服务器等方式，这种部署方式设置较为复杂、局限性较大、实现的网络管理功能有限，对网络性能的消耗较大、容易导致网络延迟等。

通过旁路的方式部署网管软件，一般是在交换机做端口镜像、部署 HUB 集线器或者代理服务器的方式，这种方式由于只能对流经端口、网卡的报文进行拷贝、识别和分析，并且也只能通过发送伪造的 TCP 报文来打断通讯，尤其是只能打断 HTTP 协议、TCP 协议的通讯，而无法有效阻断 P2P 协议、UDP 协议的报文，从而这种架构的网管系统只能限制 HTTP、TCP 协议的网页访问、电子邮件等，而无法有效阻止 P2P 下载、BT 下载、以及所有主要采用 UDP

协议进行传输的网络应用（比如网络游戏、股票软件、聊天软件等）；同时，这种架构的网管系统也只能限制电脑一段时间的流量，比如一天下载了多少兆大小的东西，而不能限制电脑实时的上网带宽、上网速度，从而也无法实现合理、均衡分配上网带宽，无法实现网络资源高效、精准、实时控制的目标。如下图所示（红叉代表这种部署方式）：

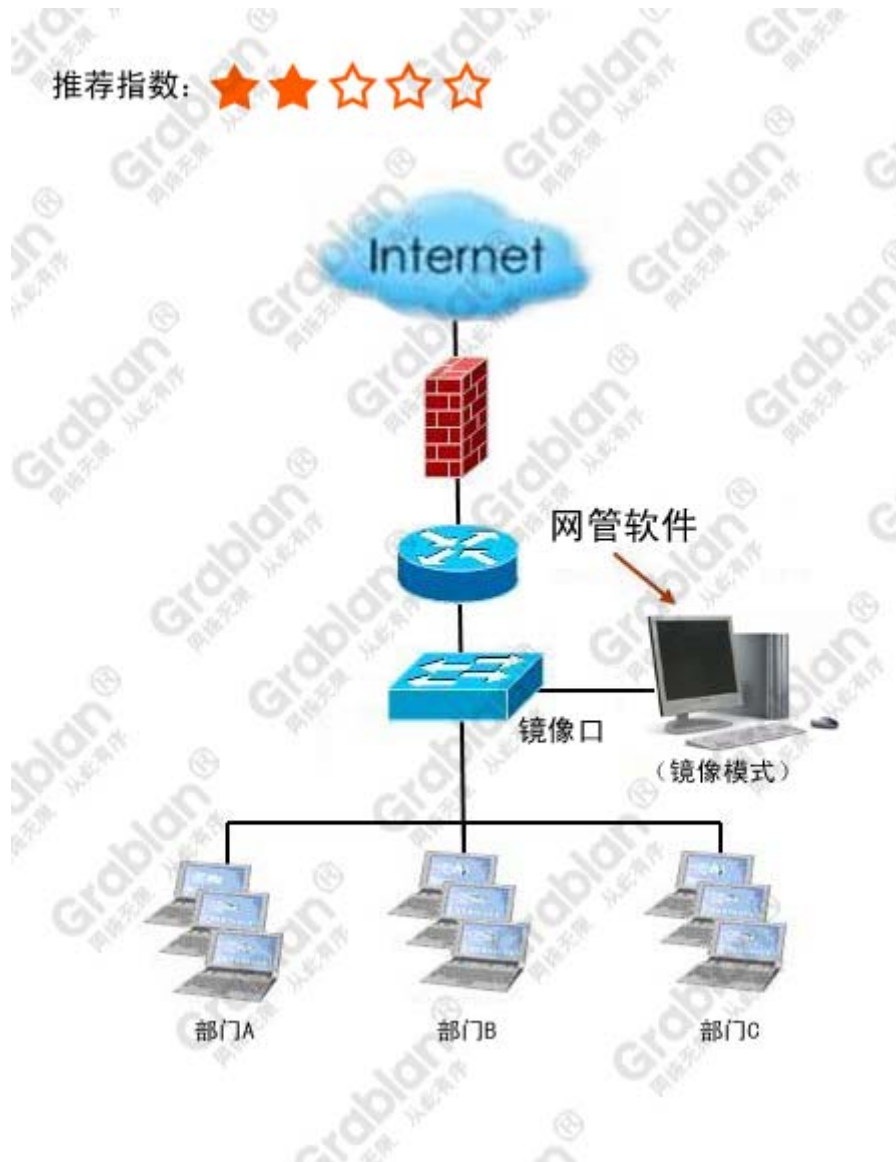


图 1：在交换机做端口镜像部署方式

推荐指数: ★★★★★

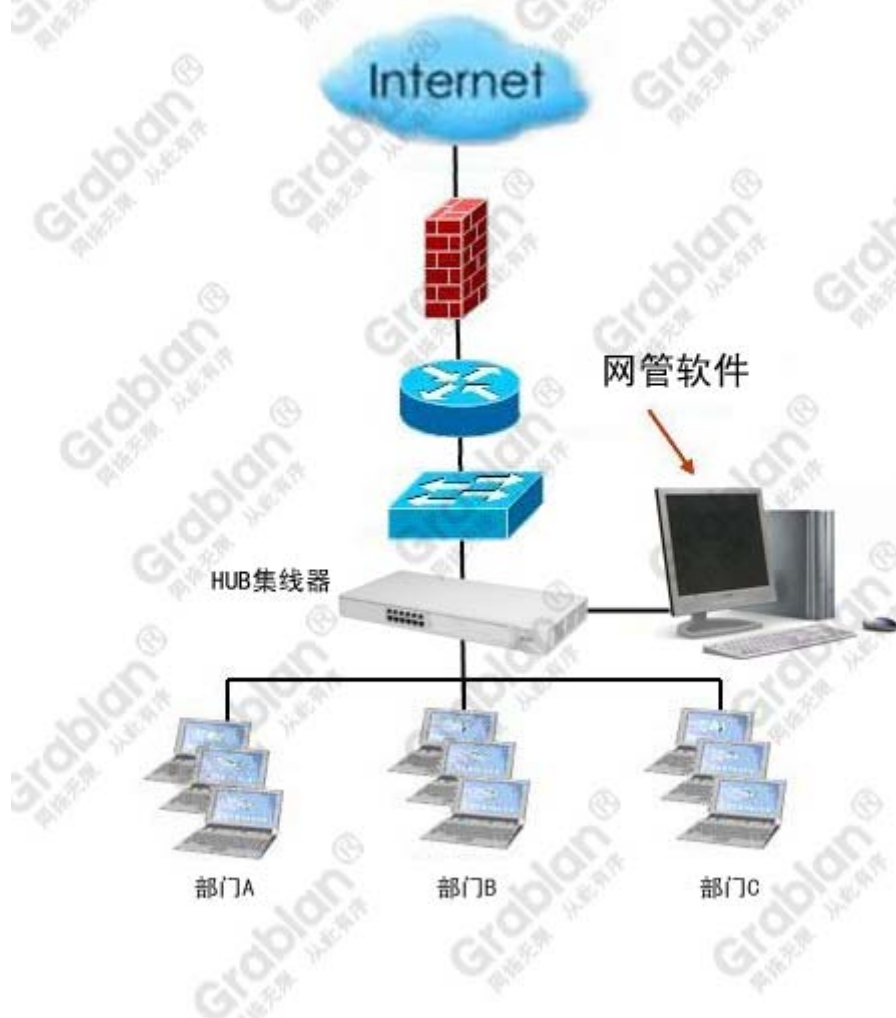


图 2：加装 HUB 集线器的方式

推荐指数: ★☆☆☆☆

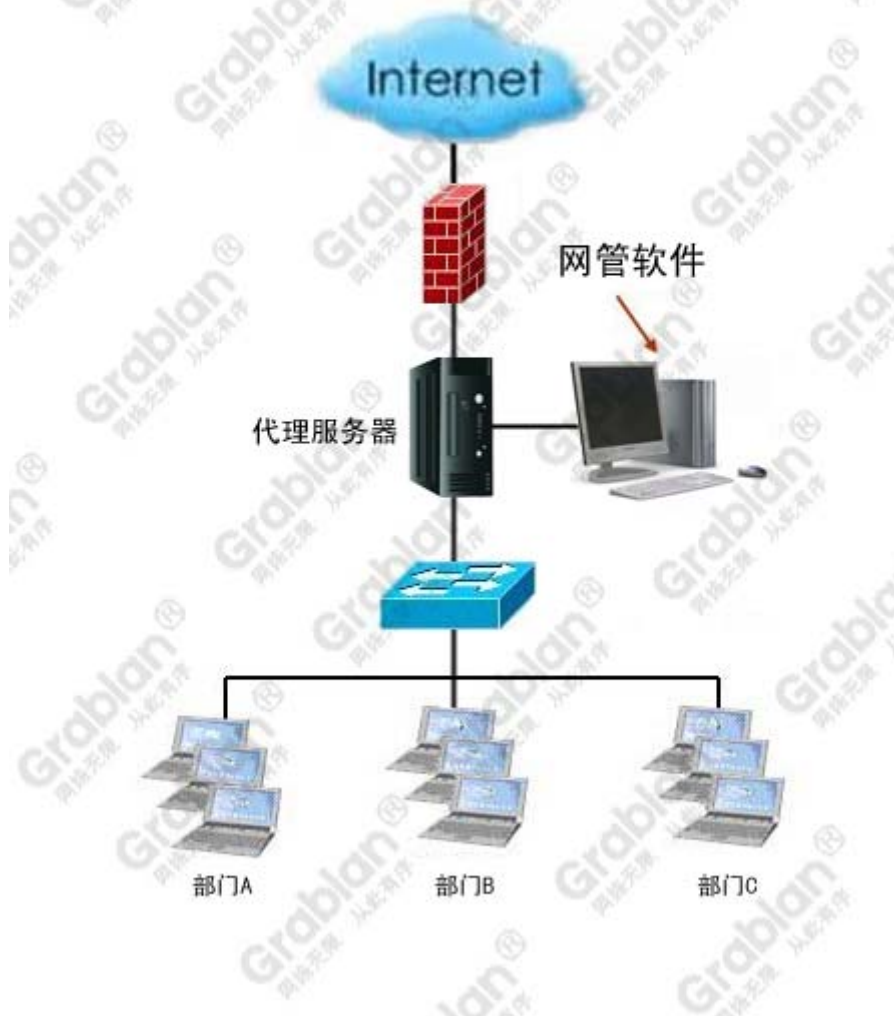
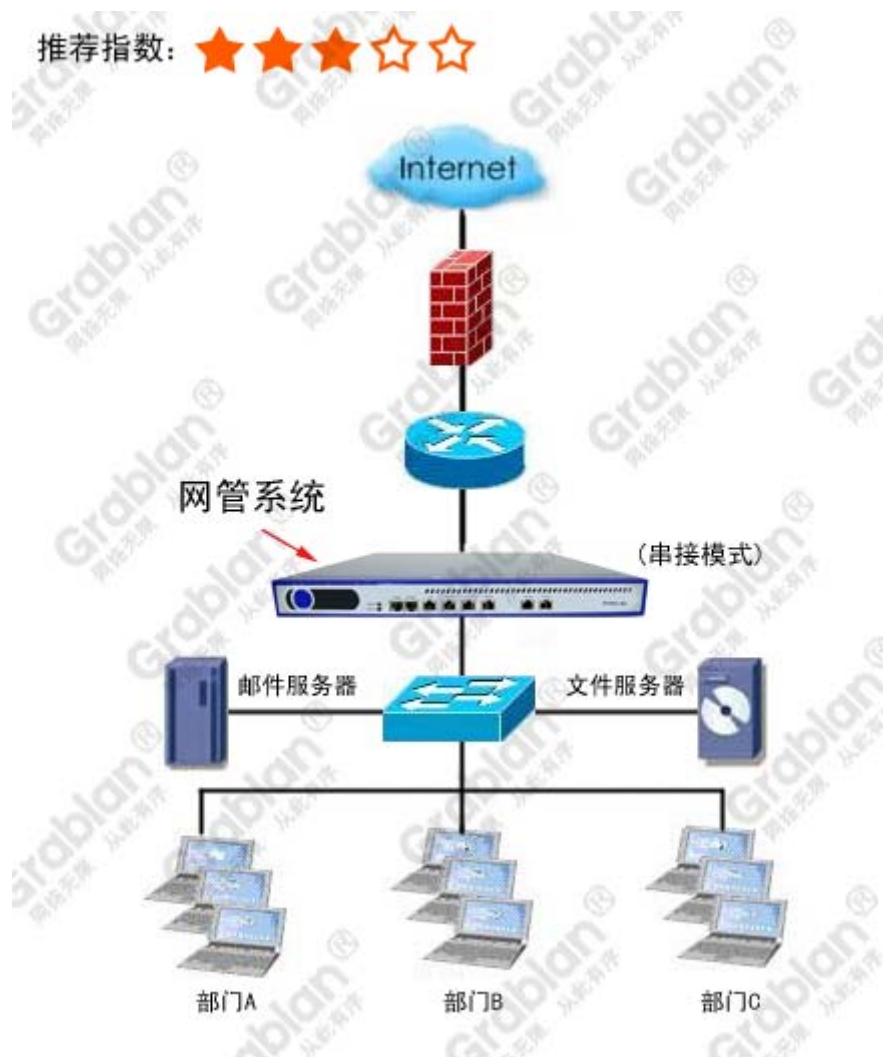


图 3:代理服务器的方式

从网管系统的发展历史来看，这种旁路架构的部署方式因为存在诸多先天性缺陷，并且存在部署繁琐（例如可能需要专门购置支持端口镜像的交换机、HUB 集线器或架设代理服务器等），并且设置复杂，自身对网络性能消耗较大（例如 HUB 集线器只能支持 10 兆，代理服务器也比较影响性能）等问题，使得这种架构的网管系统逐步退出历史的舞台。目前仅在一些需要监控上网内容，而不在意上网行为的一些小型局域网使用，不适合大型局域网环境，更不适合需要对上网行为（P2P 下载、聊天、炒股、玩游戏、限制带宽）等网络环境中使用。

二、 第二代网管系统：采用串接（桥接）部署。（当前基于硬件平台的网管系统多用此种方式部署，可以实现大部分网络管理功能，但设置较为复杂，但容易出现单点故障，风险较大，承载内网所有公网报文容易成为性能瓶颈）

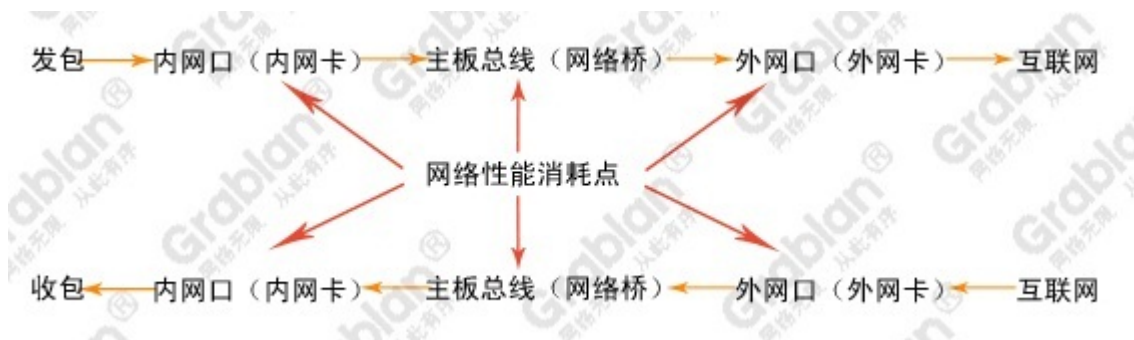
鉴于旁路方式部署网管系统面临的诸多缺憾，国内一些网管系统厂家逐步采用串接、桥接方式来取代传统的旁路模式。串接方式一般是有两个口，一个连接内网交换机，另一个连接出口网关设备，并且一般是通过双网卡桥接成“网络桥”的方式使得内网口和外网口建立连接并进行数据报文的传输，然后将网管系统部署到此“网络桥”来对过往的数据报文进行抓取、过滤、处理和转发，以此来实现对内网电脑上网行为的控制。毋庸置疑，这种方式避免了旁路模式的诸多不足，可以实现大部分的网络管控功能，但是安装部署较为复杂、风险较大、同时对网络性能消耗较大，极容易导致网络数据包延迟。如下图所示：



总体来说，这种架构的部署方式也面临以下几个问题：

首先，这种架构需要调整网络结构，三层交换机和网关设备都需要作出相应的调整，而这种调整常常是通过命令行的方式来实现的，这使得那些没有专门网管人员的单位部署起来较为麻烦，一旦监控设备出现问题，相关的网络恢复工作也较为吃力，使得这种部署方式从管理层面看，风险较大、管理较为复杂。

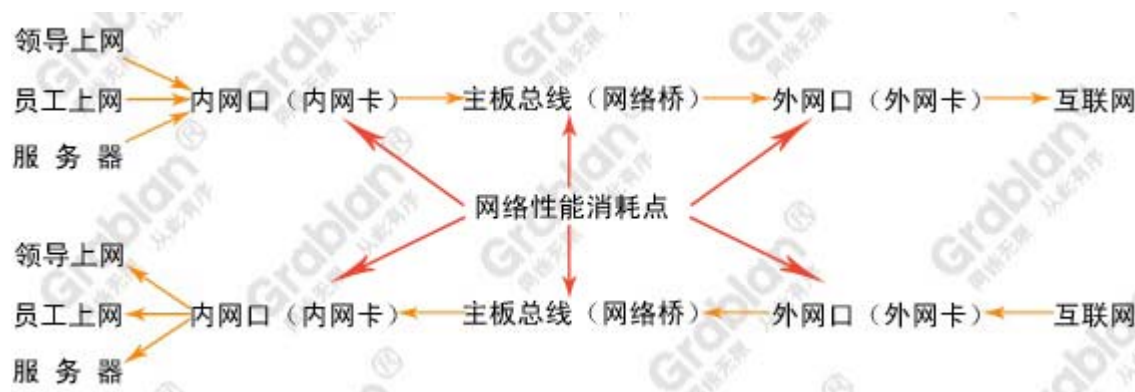
其次，由于这种监控设备的原理是通过在双网卡虚拟的“网络桥”上捕获电脑报文进行识别、过滤和拦截电脑的公网报文进而实现对电脑上网行为和上网内容的控制，而双网卡、网络桥这种方式由于数据包要经过监控设备的内网口网卡后，要通过电脑主板总线传输给监控设备的外网口网卡，然后再由监控设备外网口网卡发送到出口网关到达互联网；回来的互联网报文也是先由网关发送给监控设备外网口网卡，然后由监控设备的外网口网卡再通过主板总线发给监控设备的内网口网卡，然后再发给交换机并最终分发到局域网各个电脑上。由于局域网电脑的发包和收包每次都要经过内网口网卡、主板总线、外网口网卡的三次中转，形成三个网络性能消耗点。所以这种架构本身对网络性能消耗较大，对网速的影响较为明显，特别是网络流量较大的情况下，将导致网络延迟、中断甚至瘫痪的情况。如下图所示：



串接模式(双网卡网桥模式)下内网电脑上网收发包的流转图

再次，由于串接或者桥接的方式使得局域网所有电脑、三层交换机所有网段的电脑的数据报文都流经此“网络桥”，这就使得局域网一些关键电脑（如领导的电脑、服务器、其他免监控的电脑等）的公网报文也要经过此“独木桥”，这种的报文大量“拥挤”，极易造成性能降低、网速减慢、网络数据包延迟；同时，一旦此监控设备出现问题，将使得整个局域网电脑、三层交换机所有网段的电脑都出现断网、掉线等现象，从而也使得领导电脑或服

服务器的公网访问被中断，使得企业网络安全面临极大的风险；最后，由于一些关键电脑的数据报文也流经此网络设备，从而使得单位的商业机密、重要文件面临着被嗅探、捕获和泄密的风险，从而对企业的稳健经营产生重大隐患。如下图所示：



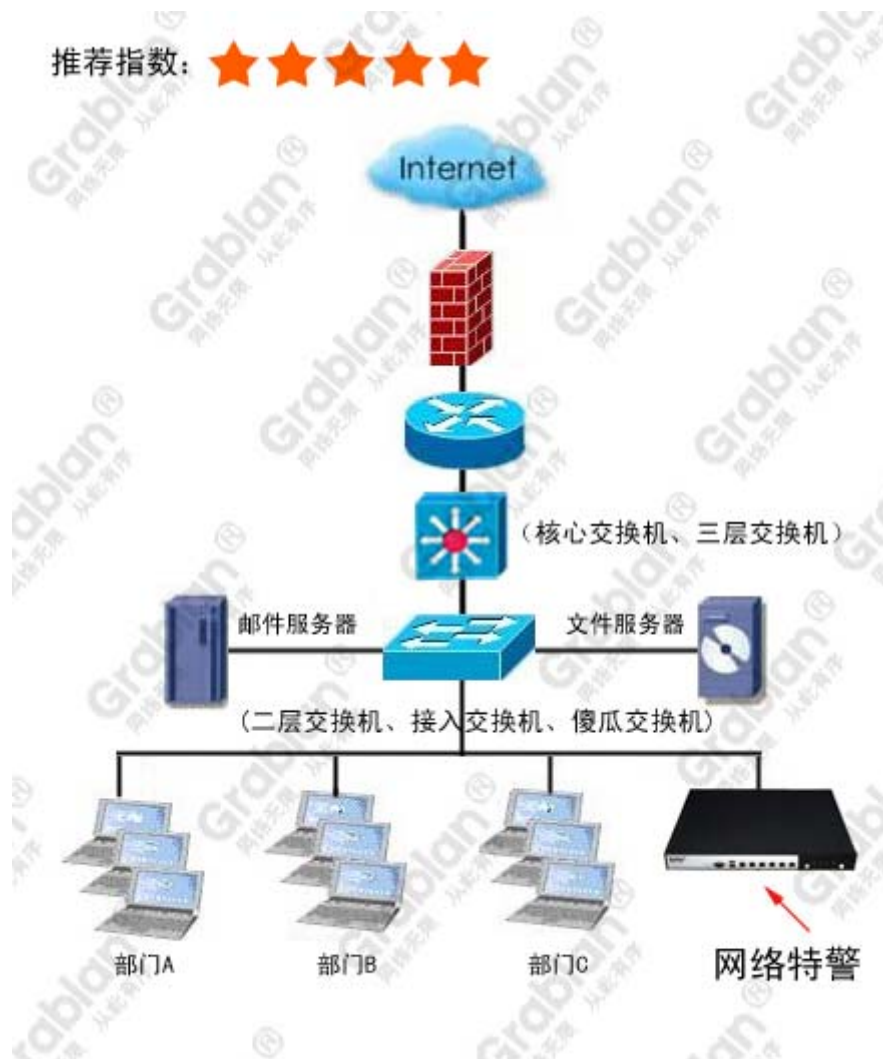
领导电脑、服务器和员工电脑的公网收发报文都经过网管设备的流转图

最后，由于这种网络监控设备是部署在三层交换机和出口网关设备之间，这使得一般的监控设备无法获取三层交换机各个网段内的电脑的 MAC 地址，而只能获取三层交换机出口接口的 MAC 地址（也即你看到局域网各个电脑的 IP 都对应同一个 MAC 地址的情况）。这使得一旦某个网段内的电脑更改自己的 IP 地址成为另一个 IP 地址（尤其是普通员工、外来人员将自己的 IP 地址更改成领导的 IP 地址以获取更高的上网权限）后网管系统将无法识别，从而一方面容易造成 IP 地址冲突，网络管理失效，另一方面也容易导致内网商业机密和关键信息的丢失、被盗，从而使得内网安全和商业机密面临极大的风险。

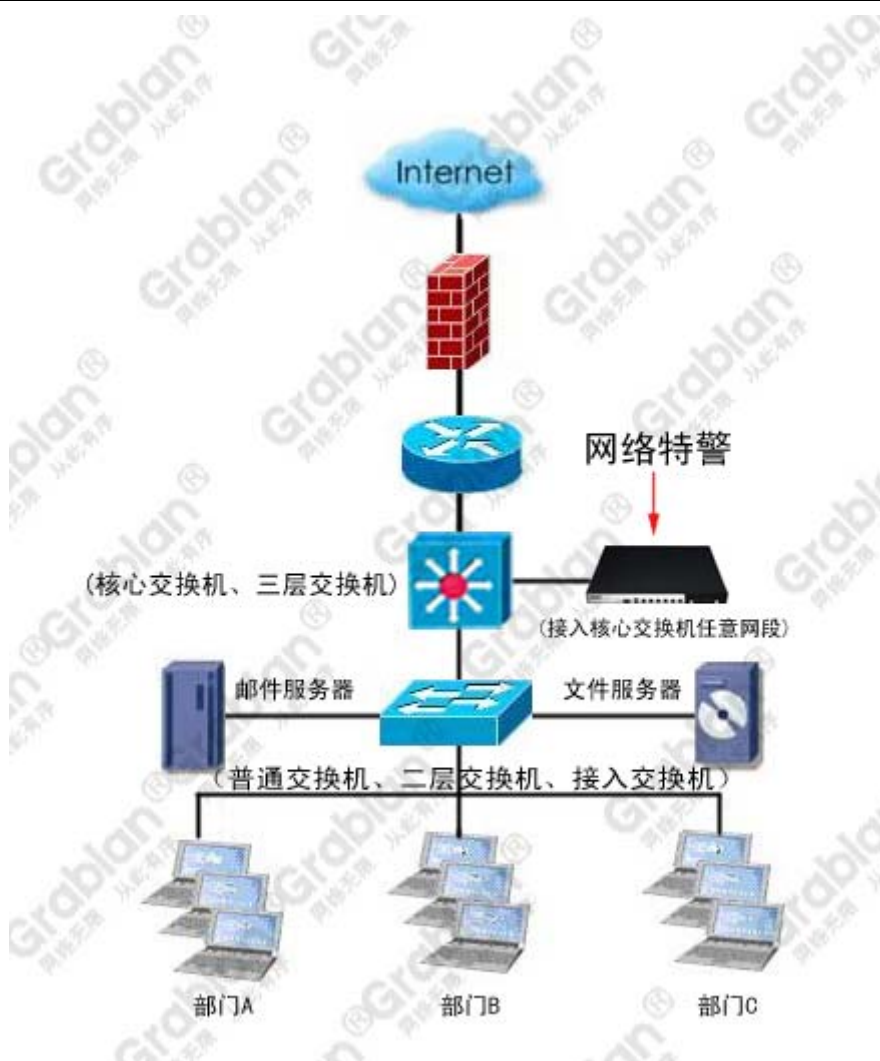
综上所述，这种串接、桥接的网管系统由于承载着本地局域网所有公网报文，关系着网络的稳定、安全和畅通，因此对其稳定性、安全性有了更高的要求，否则一旦出现问题，将对局域网造成较为严重的影响；同时，由于这种部署方式由于一般无法获取客户端的 MAC 地址或者主机名，因此无法精确定位、约束被控制的电脑，造成无法有效实现网络管理的目的。

第三代网管系统：基于“创新直连”架构的部署方式（网络特警引领网管系统未来发展趋势的部署方式，安装部署极为简单，可以实现所有的网络管理功能，全透明部署，不会出现单点故障，不需要调整任何结构或加装任何设备，超高速转发数据包，不会出现性能瓶颈，不会导致网络延迟）

鉴于采用旁路模式和串接模式部署网管系统面临的一些不足，以及用户对于高可靠性、高安全性、更快捷部署、更简单设置网管系统的强烈需求，并且通过对当前最新网络管理技术的深入研究和大胆突破。大势至（北京）软件工程有限公司推出了基于“创新直连”架构的网络特警上网行为管理系统，通过直接连接二层交换机或者三层交换机的任意网段的任意一个端口即可实现对局域网全部电脑、三层交换机所有网段电脑的全方位监控，一举解决了当前硬件架构网管系统通过串接、桥接的各种不足，可以实现更安全、更精确、更智能、更快捷的网络管理。具体部署如下图所示：



网络特警可以直接部署在二层交换机、普通交换机的环境



网络特警可以接入划分 VLAN 的交换机的任意网段内

基于“创新直连”架构的网络特警上网行为管理系统，通过深入研究交换机传输原理和互联网基础通讯协议的基础上研发成功的。“创新直连”的具体含义如下：

- 1、通过网络特警硬件平台自带的单块高性能网口直接连接交换机或者路由器。不论是二层交换机、还是三层交换机、甚至是核心交换机，即可实现对下面所有网段、所有电脑的上网行为的全面控制。同时，也只需要连接交换机，而不需要连接出口网关或者其他设备，也不需要网络做出任何调整或加装任何其他网络设备。
- 2、网络特警采用单块网卡进行抓包、识别、过滤和转发。网络特警直接从网卡高速缓存抓取数据包进行处理，处理完毕之后直接放入网卡高速缓存，网卡通过内部集成的高速芯片(峰

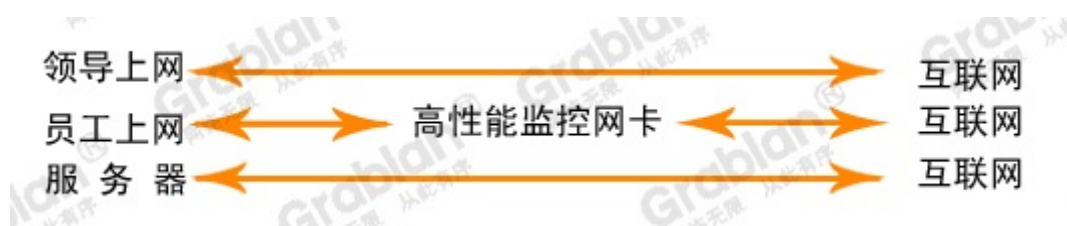
值传输速度可以达到 2.5G，远超主板总线传输速度）直接将数据包发送到公网出口，而不是给监控设备的主板总线和另一块网卡，从而避免了网络数据包的多次中转、来回公网报文都要中转对网络性能的消耗，大幅度提升了监控效率，避免了网络延迟。如下图所示：



网络特警数据包流转图

3、基于单向监控的模式下，下行数据包由出口网关直接发送到交换机并最终分发给局域网相应的电脑，这样下行的网络数据包不需要再流经网络特警监控设备，考虑到下行包常常远大于上行包，尤其是局域网某些情况下常常用 P2P 软件（如迅雷等）下载大的文件，从而可以更进一步避免网络延迟，同时也极大地降低了监控设备的负荷，提升了网络特警的监控效率。

4、对于局域网一些免监控的电脑，如领导或服务器等主机的公网报文，通过简单设置，即可完全不流经网络特警的监控设备，而是直接通过交换机发送到出口网关到达互联网，而回来的互联网报文由网关直接发给领导电脑和服务器。由于领导电脑和服务器的公网数据包不流经网络特警的监控设备，从而一方面降低了监控设备负荷，避免了公网报文的拥堵排队情况；另一方面也避免了监控设备出现单点故障可能影响领导上网或者服务器关键业务出现中断的风险；最后，由于领导或服务器的公网报文不流经网络特警监控设备，从而也使得这些重要电脑的数据报文不会被监控设备等第三方设备捕获，有利于保护信息安全和商业机密！如下图所示：



网络特警免监控电脑数据包和被监控电脑（如员工电脑）流转图

5、安装部署方式同时向下兼容，可以适应国内各种网络环境，是国内监控模式最多的硬件行为网关系统。也即，网络特警也可以完全采用旁路方式（连接交换机镜像端口、HUB 集线器或代理服务器来进行部署）；也可以完全按照串接、桥接模式进行部署，并可以实现上述部署方式下所有其他软硬件网管系统所能实现的所有功能，从而可以满足某些客户的特定网络结构和特殊网络管理需要。

6、全透明安装，支持热插拔网络自动导通。在某些不需要监控的情况下，可以直接停止监控设备的工作，甚至可以将监控设备直接移除，网络即可自动、智能恢复，从而极大地降低了特殊情况下的网络通讯风险。

总之，网络特警基于五个方面的“直连”技术，不但避免了传统部署网管系统的复杂性、网络性能消耗、数据包延迟、单点故障风险等诸多不足和缺陷，而且还大幅度提升了监控设备的监控效率、优化了整体网络性能、降低了部署网管设备的复杂性和工作量，而且可以进一步保护企业信息安全和商业机密，从根本上保证网络的安全、稳定和畅通。

网络特警“创新直连”架构的诸多优势汇总如下：

1、安装部署最快捷、最简单、工作量最小、最安全

网络特警上网行为控制系统直接连接局域网二层交换机、普通交换机、三层交换机或者核心交换机的任意网段的任意一个端口，即可实现对二层交换机所有电脑、三层交换机、核心交换机所有网段电脑的全面监控，从而可以不需要调整网络结构，不需要对三层交换机、网关设备等做任何调整，不需要在三层交换机做端口镜像、部署 HUB 集线器或者代理服务器的情况，极大地降低了部署网管系统的复杂性、工作量；同时，这种监控模式也不会对网络安全造成影响，保证了网络的持续、稳定、高效运行。

2、内有乾坤、硬件按需定制、同类产品性能最高

网络特警上网行为管理系统内置英特尔高性能数据转发专用网卡（本网卡基于 PCI-E 技术架构，标配传输速率在 2G 以上，高端设备内置 10G（万兆）速率网卡，可以满足国内所有企事业单位的需要），不需要两块网卡搭建网络桥，从而避免了“网络桥”对网络性能

的消耗，极大地降低了部署网管系统的负面影响和对局域网的拖累，同时稳定性更高；同时，为了满足不同用户的对硬件监控系统的扩展、冗余需要，我们提供了针对用户环境的硬件个性定制、无偿升级的策略，从而不仅可以满足用户当下的网络管理需求，而且可以满足用户未来较长时间的硬件性能需要，性价比更高。与国内其他基于硬件架构的上网行为管理系统一般不公布（或者不好意思公布，因为他们的配置太低，CPU 一般用 Atom、赛扬、奔腾等低端 CPU, 内存一般用容量较低的一代内存等）具体硬件配件参数不同，网络特警全线产品的最低配置、高端配置如下表所示：

CPU	内存	硬盘	网卡
酷睿 2 双核	4G DDR2 以上	500G	英特尔 PCI-E 千兆网卡

网络特警最低配置表

CPU	内存	硬盘	网卡
i5-i7 多核/至强多核	4G -16GDDR3 以上	1TB-2TB	英特尔 PCI-E 万兆光网卡

网络特警高端配置表



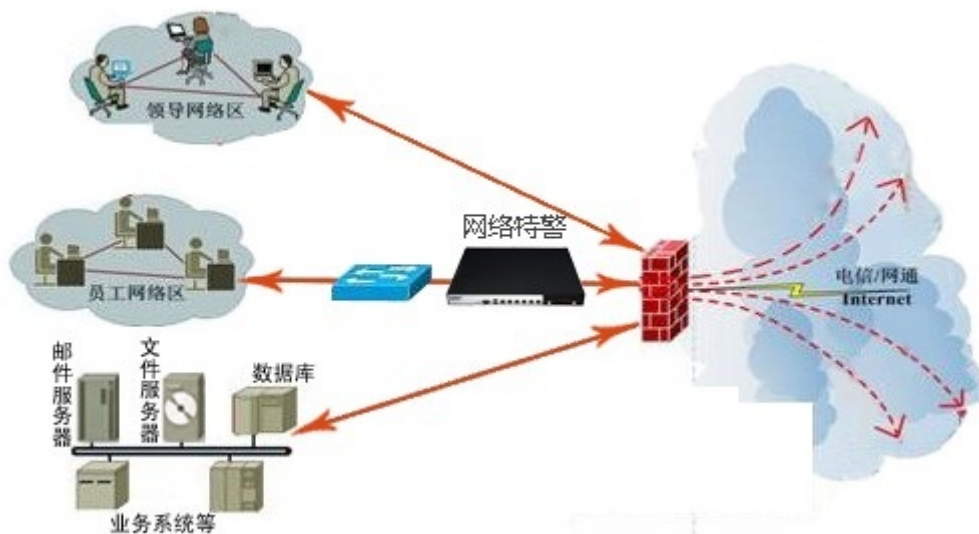
网络特警外观

平台架构	标准 1U/2U 工业设计，高强度钢外壳
CPU	支持 Intel Core i3/i5/i7
内存	4G-16G, DDR3/1333MHZ
硬盘	500G-2TB 高速 SATA 硬盘
网卡	Intel PCI-E 高性能千兆/万兆网卡
LAN BYPASS	2 组
峰值流量	10G
工作温度	0-60°

网络特警平台参数

3、免监控的电脑公网数据包不流经网络特警监控设备，从根本上保证了信息安全、商业机密，最大限度降低设备负荷，提升监控效率，彻底避免导致网络延迟现象。

网络特警上网行为管理系统由于直连三层交换机，并可以识别三层交换机的各个网段的电脑，从而可以对重要网段、重要电脑或者服务器免于监控。这种免于监控也不同于其他网管设备的“免监控”，而是基于以下两个方面：一方面，免监控的网段、电脑或者服务器的公网报文根本不流经网络特警上网行为管理设备，而是直接通过三层交换机发送到出口网关，从而避免了和被监控的电脑的公网报文一起“排队”等待过滤转发的情况，避免出现报文拥堵、丢包和延迟的现象，正如根本没有部署网管系统一样（而同类的网管设备，由于采用串接、桥接等方式，从而使得即便是免监控的电脑或服务器的公网数据包也被迫必须流经监控设备，加大了数据包的拥堵，导致网络延迟增大，网络性能下降，监控设备负荷增加）；同时，由于领导或关键服务器的数据包不流经网管设备，从而避免了被第三方工具嗅探、截获商业机密的情况，从而也极大地保护了信息安全和商业机密；另一方面，相应地，由于免监控的主机公网报文根本不流经网络特警监控设备，从而即便设备出现故障也不会影响到这些免监控网段、电脑或者服务器的正常运行，从而可以保证企业内部关键业务的永续进行不受干扰。如下图所示：



网络特警免监控电脑数据包和被监控电脑（如员工电脑）模拟图

4、跨三层交换机进行 IP 和 MAC 地址绑定、策略和主机硬件绑定，从而保证监控精准定位、无处可逃

由于网络特警监控设备直接连接三层交换机或者核心交换机，从而可以轻松获取三层交换机各个网段、各个电脑的 IP 和 MAC 地址对应关系，网管人员可以进行 IP 和 MAC 地址（从而避免了使用三层交换机做 IP 和 MAC 地址绑定的繁琐），同时由于可以将主机上网策略和其 MAC 地址进行绑定，从而无论被控制的电脑如何更改 IP 地址仍旧在网管先前指定的上网策略下上网，从而杜绝了客户端电脑或者外来电脑企图通过修改 IP 地址逃避监控、获取更高上网权限的行为，极大地保护了企业的内网安全和保护了商业机密，实现了更为严肃、精准的网络管理。

5、“心跳”技术实时跟踪、智能、自动、多手段迅速恢复网络

首先，网络特警和聚生网管系统一样，如果在监控过程中，程序因为自身的 BUG 或者病毒的破坏等原因而导致网络特警停止工作，那么这种情况下，网络特警的守护程序会自动关闭网络特警并重新启动，从而可以保持网络监控永不中断，保证网络的稳定、安全和畅通。其次，由于网络特警上网行为监控系统直接连接三层交换机进行监控，一旦不再需要监控或者监控设备出现故障，网络特警上网行为监控系统将自动启用 Bypass 功能恢复网络，这种

情况下网络将自动恢复到原初的状态，就和之前从未部署网管系统一样；同时，你也可以直接重启三层交换机即可迅速恢复网络；此外，网络特警上网行为监控系统还提供了额外的防护机制，网管人员可以在自己的电脑通过运行大势至公司提供的网络恢复工具即可迅速恢复网络，保证网络的在 10 秒以内即可轻松恢复；最后，网络特警还可以在特定条件下自动重启操作系统、自动登入操作系统并自动重新启动，从而可以保证长期运行的情况下，网络特警的安全、稳定和高效。

6、根据客户合理化需求进行个性化、实时定制功能，确保网络管理可持续发展

中国企事业单位网络结构各种各样、网络需求各不相同，因此单一的网络管理系统无论多么强大，也无法满足客户的个性化需求，而向网管系统厂商要求个性化定制常常需要付出高额的费用——和客户一样，我们始终无法理解，为什么一个简单的网络管理功能，网管系统厂商要向客户索取高额的定制费用。为此，我们提出了“网络所需 我们所能”的这一公司宣言，这也是我们对客户的庄严承诺！——所以，确切地说，你并不是购买一套“网络特警”上网行为管理系统，而是购买一种实时的、个性化、按需定制服务，这种服务的初衷和最终目的只有一个，那就是：满足客户的个性化、全方位、真正的网络管理需要，为客户创造网络切实的网络管理收益，保证你的网络管理可持续发展。

7、模块化设计、模块化部署，最大程度降低系统负荷、最大限度提升性能

我们常常看到国内某些网管软件厂商宣称自己的产品可以完美地提供“一站式、全功能”的解决方案：集成网关路由功能、防火墙、代理服务器功能、网络访问行为管理、邮件安全与杀毒、流量管理、阳光上网、网络监控、VPN 功能等等，几乎涉及到网络安全、网络管理、网络监控、网络行为的一切方面，给人的感觉十分强大、无所不包。但是实际的情况是，就目前国内网络管理软件厂商的技术实力、研发实力还是资金实力而言，都无力研发这种“无所不能”的网络管理系统；即便是国外的网络公司也没有这种“一站式”的产品，所以我们总会看到不同的网络管理产品总是专注网络管理的某个特定方面，有的专注于信息安全、有的专注于网络行为管理、有的是专门的防火墙，当然也有专门的杀毒软件。所以当有厂家宣称可以提供“一站式”的方案的时候，作为客户要小心了，一个产品如果什么功能都可以实现，那么它的每个功能都不可能完善，这种情况下，客户最需要的功能往往也不能很好地满足，而只有专注于某一领域的厂商才可能提供更为专业的产品。所以，无论是早期的“聚

生网管”还是如今的“网络特警上网行为管理系统”，我们总是专注于最核心的网络管理功能，帮助客户实现最重要的应用价值。同时，网管系统越复杂，其对网络数据包的抓包、分析、过滤、转发等步骤就越多，网络消耗就越严重，监控效率也就越低；同时，越庞大的网管系统由于代码量更大、隐含着更多的 BUG，会导致系统的稳定性更低。为此，和你见到的其他网管设备不同，网络特警上网行为管理系统仍旧是一款专业的网络监控设备，仍旧专注于员工上网行为管理；另一方面，根据用户的某些特殊网络管理需求，我们开发了很多网络管理插件，这些工具可以独立运行，从而避免拖累网络特警上网行为管理系统，又可以帮助用户实现个性化、特殊的网络管理需求。

8、操作系统平台优势，支持 Windows 操作系统和 Linux 操作系统，扩展性大大增强

网络特警上网行为管理系统同时支持基于 Windows 平台的 X86/64 位操作系统，同时也支持基于 Unix 和 Linux 操作系统，同时还支持虚拟机运行网管系统，从而可以满足用户多层次、多平台的网络管理需要；同时，网络特警上网行为管理系统也可以以软件形态单独运行，从而可以直接运行在客户现有的服务器、高性能主机上，从而便于充分利用用户现有的硬件平台和操作系统，减少资源闲置和浪费状态。这样一方面降低了用户的采购网管系统的支出，同时也便于用户利用现有的软硬件平台运行网管系统实现网络管理的目的，并且还有利于用户降低电能消耗、实现低碳环保的网络管理和网络监控，从而帮助用户实现最具性价比、最具经济效益的网络管理。

网络特警™上网行为管理系统详细功能介绍

网络特警™上网行为管理系统是大势至（北京）软件工程有限公司在充分总结聚生网管系统八年网络管理实践和经验，并深入调查各行业用户的网络管理需求、充分集成当前最新的网络管理技术的基础上推出的一款基于硬件嵌入式芯片的网络管理系统。网络特警™上网行为管理系统以最有效限制 P2P 下载、限制聊天软件、控制上网带宽、限制股票软件、限制网络游戏等为第一核心网络管理功能；以记录邮件内容、记录聊天内容、记录 FTP 文件传输内容、监控对方屏幕和进程、监控留言和发帖等内容监控为第二核心网络管理功能；以有效防御 ARP 攻击、抵御广播风暴攻击、禁止代理上网、限制外来电脑接入内网、IP 和 MAC 地址智能绑定等为第三核心网络管理功能。通过将三大核心网络管理功能进行有效的整合、协同，使得网络特警™上网行为管理是当前国内网络管理功能最全面、最实用、最有效、最简单的专业网络管理系统。同时，大势至（北京）软件工程有限公司通过基于用户网络环境和网络管理个性化需求的按需定制服务，可以确保用户既能实现共性的、常规的网络管理，又可以实现个性化的网络管理，使得用户真正实现网络管理的目的，为企业事业单位创造最大的网络管理收益和经济效益。

网络特警™上网行为管理系统详细功能如下：

一、完全控制 P2P 下载、普通 HTTP 下载和 FTP 下载

- 1、P2P 下载控制功能：可以控制如 BT、eMule(电驴)、百度下吧、PP 点点通、卡盟、迅雷等高达 15 种 P2P 工具的下载。
- 2、P2P 视频传输的功能：可以拦截如 PPFilm、PPVod、QQlive、沸点网络电视等等高达 12

种当前流行的 P2P 视频工具。

- 3、P2P 下载智能带宽抑制功能：当发现有主机进行 P2P 下载时，自动降低该主机可用带宽。
- 4、HTTP 下载控制功能：用户可以自行设定控制任意文件下载，也可以指定文件后缀名限制下载。
- 5、FTP 下载功能：用户可以自行设定控制任意文件下载，也可以指定文件后缀名。
- 6、系统可以禁止一切 HTTP、FTP 的上传下载。

二、有效限制电脑上网带宽（流速）、上网流量

- 1、实时查看局域网主机带宽占用：从大到小排序功能使得网管可以对网络占用了然于胸。
- 2、针对特定主机分配公网带宽：可以使企业有限的公网带宽得到最充分的利用，从而使得某些主机无法再大量消耗带宽。
- 3、主机报文数据分析功能：使得网管可以知道主机所占带宽是用于什么应用。
- 4、系统可以为局域网主机设定上行、下行流量和总流量，超过设定流量，自动断开其公网连接。
- 5、流量每日自动清空的功能，用户可以根据需要选择。

三、有效限制 QQ、MSN 等国内流行的聊天软件

- 1、网络特警™上网行为管理系统可以封堵的聊天软件有：QQ, MSN, 网易泡泡, 新浪 UC, QQ 传文件, MSN 传文件, AIM(ICQ), Skype 网电话, SoQ 搜 Q, 阿里旺旺, 雅虎通, IRC, 飞信等等；特别是在控制方式上，网络特警™上网行为管理系统只需点点鼠标就可以封堵 QQ、SKYPE 等国内其他网管系统一般无法封堵的聊天软件，特别是封堵 SKYPE 网络电话，在国内外都居于领先地位！
- 2、系统可以禁止 QQ、MSN 文件传输，保证客户信息安全。

四、局域网主机 IP 和 MAC 的绑定功能

针对局域网用户经常私自更改 IP，导致局域网 IP 地址冲突或者通过私自更改 IP 获取对局域网的更高的访问权限的功能，网络特警™上网行为管理系统系统集成了 IP 和 MAC 智能

绑定功能，可以对局域网主机进行个别、批量或者全部绑定，绑定之后，局域网电脑如果私自更改 IP 之后，就会无法访问网络，并且网络特警™上网行为管理系统系统还可以发送人性化的警告信息，告知其默认的 IP 是什么，必须修改回默认 IP，否则将无法访问网络，从而可以规范网络管理；同时，网络特警™上网行为管理系统还可以自动发现新主机并自动进行 IP 和 MAC 绑定，从而可以简化网管的工作，实现智能、自动化管理！

五、当前所有流行网络游戏的控制功能

网络特警™上网行为管理系统目前集成了 20 余种当前最流行的网络游戏，如禁止泡泡堂、QQ 游戏、边锋游戏、浩方游戏、POPO 游戏、中国游戏中心、同程游戏、youxi518 游戏、youxi8848 游戏、38game 等游戏、联众游戏、上海热线等等。同时，还可以根据客户的需要定制特定网络游戏的控制规则。

六、当前所有流行股票软件的控制功能

网络特警™上网行为管理系统目前集成了 10 多种当前最流行的股票软件控制规则，如大智慧(包括大智慧新一代)、同花顺、广发至强版、龙卷风行情分析软件、钱龙旗舰、国元证券软件、分析家、麒麟短信王、光大证券超强版、证券之星、国信证券、申银万国等等。同时，还可以根据客户的需要定制特定股票软件的控制规则。

七、当前所有在线游戏网址的控制功能

当前越来越多的网络游戏通过网页的形式就可以直接打开，而且这些在线游戏大多采用 P2P 连接技术，对网络带宽的占用十分惊人。网络特警™上网行为管理系统目前集成了当前国内流行的 100 种以上的在线游戏的网址的控制功能，管理员可以点点鼠标就可以封堵当前所有流行的在线游戏网址，并且可以随时扩展，实时控制最新的在线网络游戏。

八、当前所有在线视频网址的控制功能

随着在线视频的日渐流行，观看在线视频是当前局域网用户访问因特网的一个重要行

为，这些在线视频大多采用流媒体技术，并且还融合了 P2P 技术，使得在线视频对带宽的占用也十分客观。网络特警™上网行为管理系统集成了当前主要的在线视频网址的控制功能，可以控制高达 30 余种当前最具人气的在线视频网址，点点鼠标就可以完全控制对这些网址的访问，从而杜绝了局域网用户过量观看在线视频对带宽的大肆占用。

九、局域网主机强制隔离功能

网络特警™上网行为管理系统集成了对局域网危险主机的强制隔离功能，当网络特警™上网行为管理系统发现局域网某些主机遭遇蠕虫、冲击波等病毒攻击时，网络特警™上网行为管理系统会自动将其隔离，被隔离的电脑将中断对局域网其他主机的访问，避免感染其他电脑或服务器，防止危害整个局域网；同时，被隔离的电脑也将中断访问因特网，防止病毒运行时对带宽的大肆占用，发送垃圾数据报文堵塞网络的风险！

十、集成了访问控制规则(ACL)功能

系统为网管人员提供自定义控制接口-ACL 规则设置，通过 ACL 规则，你可以设置包括 IP 源地址、IP 目标地址、协议号（TCP/UDP）、端口范围等参数的规则，系统将自动拦截符合规则的数据报文，通过使用 ACL 规则，你可以轻松的实现控制功能的灵活扩展。如控制局域网任意主机 IP 对任意公网 IP 的访问；控制任意的聊天工具、控制任意的网络游戏等等。目前网络特警™上网行为管理系统系统已经预设了高达 10 余种各种访问控制规则，并根据客户的需求不断增加。

十一、禁止局域网用户访问共享资源

当前在有些企事业单位的网络管理中常常遇到这样的情况：外来的电脑私自接入单位内部的局域网，访问未经授权访问的共享资源以及服务器的关键资料，这些信息的泄露将给企事业单位带来巨大的损失。针对这种情况，网络特警™上网行为管理系统集成了对外来主机访问共享资料的自动限制功能，这样，私自接入到单位内部局域网的外来电脑，即便各项设置都正确，也无法访问共享资源，并且这种限制是全自动、无人值守的情况下完成的，从而有力地保护了企业关键数据的安全；同时，网络特警™上网行为管理系统还提供了监控访问

共享资源访问的功能，比如在服务器上运行网络特警™上网行为管理系统提供的共享文件查看器，就可以记录局域网电脑访问服务器共享文件，包括拷贝、删除、创建、修改的所有记录，从而便于网管人员审计信息安全，防止无关人员盗取公司重要文件的行为，同时也便于事后调查取证。

十二、网址浏览管理

网络特警™上网行为管理系统集成的网址控制功能包括白名单和黑名单。管理员可以添加任意某一个网址做为白名单，则局域网任意主机只能访问此网址及其所有的二级页面；管理员也可以设定某一个单一的页面，作为白名单，则局域网主机只能访问此单一设定的页面；管理员可以设定某一个网址的某一个频道作为白名单，则局域网主机只能访问这个网站的这个频道主页及其频道内的所有二级页面。如果管理员设定某一个网址为黑名单，则这个网址的主页及其所有的二级页面都将被完全禁止；如果管理设定这个网址的某一个页面为黑名单，则局域网主机就不能访问此页面，但可以访问其他所有的页面；管理员也可以设定网站的某一个频道为黑名单，则这个网站的这个频道的主页及其所有的二级页面都不可以被访问，但不影响局域网主机访问其他的所有频道和页面。

十三、邮箱访问控制

当前很多企事业单位没有自己的企业邮箱而普遍使用门户网站的免费或收费邮箱，但是企事业单位不希望客户端借访问邮箱的机会而点击门户网站的新闻、娱乐等与工作无关的网页访问行为。针对这种情况，网络特警™上网行为管理系统集成了对门户邮箱的访问控制功能。具体如下：

- 1、可以指定局域网的电脑只能访问某个或者某些邮箱而不能打开与邮箱无关的网址。
- 2、系统目前集成了对 sina、163、sohu、yahoo、21cn、hotmail 等等当前主流的邮箱控制功能

十四、局域网主机异常的警报功能

网络特警™上网行为管理系统通过集成的警报工具，可以实时侦测局域网关键服务器、工作站的运行状况。当这些关键服务器、工作站出现异常时，警报工具会通过手机短信、邮件等方式通知网络管理员，便于采取紧急修复、维护，防止出现关键应用中断而无人得知和响应的状况，保证关键业务的不间断运行。

十五、局域网主机远程开机、关机、重启、注销功能

通过网络特警™上网行为管理系统集成的远程管理工具，不需要在客户端安装任何件，网管人员可以实现对局域网电脑(单个或者批量)进行远程开机、远程关机、远程重启、远程注销等操作，方便了内网管理。

十六、控制局域网主机对光驱、软驱、USB 的使用

网络特警™上网行为管理系统系统还提供了对局域网主机的光驱、软驱、USB 的访问控制，从而可以防止未经授权的用户私自用光驱、软驱、U 盘、移动硬盘拷贝公司的相关资料，防止重要信息的外泄。

十七、监控通过网页发送的 WEB 邮件、发帖、留言（注：此功能需要扩展插件）

系统可以详细记录并限制通过网站所发的 WEB 邮件（包括内容和附件）、发帖、留言等通过 HTTP 外发的内容。

十八、监控 Outlook、Foxmail 等邮件收发的邮件内容（注：此功能需要扩展插件）

可以详细记录并限制通过 Outlook、Foxmail 等各种邮件收发工具接收和发送的邮件（包括内容和附件）。Netsense 可以根据需要对电子邮件进行监控，不仅可以知道邮件的去向、大小、何人所发，还可以截获电子邮件的内容，这可以有效地阻止通过电子邮件获取企业机密的行为。

十九、可以详细记录并限制通过 FTP 工具上传和下载的文件（注：此功能需要扩展插件）

文件传输方式（FTP）也是获取内部网络机密常用的手段之一，现在上网速度越来越快，小到几兆，大到几十兆、上百兆的信息都可以在短时间内上传出去，这对企业的信息安全有着巨大的威胁，必须进行实时监控。网络特警™可以自动对 FTP 的各种行为进行监控与记录，非常实用。

二十、网络限制功能管理

- 1、WWW 访问完全控制：网管可以选择是全部禁止上网还是使用过滤规则上网。
- 2、黑白名单规则：网管可以设定网址过滤规则，支持黑白名单自定义。
- 3、色情网址过滤：系统可以自动过滤符合色情网址库的访问。
- 4、局域网主机充当代理服务器控制：系统可以自动限制局域网主机充当代理服务器，以禁止不当局域网扩展。
- 5、局域网使用 WWW 代理控制：禁止局域网主机使用 Socks 等代理访问 WWW。
- 6、系统可以精确、完整记录主机所上网站，便于事后审计。

二十一、组策略（上网权限）管理功能

- 1、可以为局域网所有主机建立统一的控制策略。
- 2、可以按照局域网主机设置不同的策略。
- 3、各个控制策略组里面的主机可以在各个不同的策略之间灵活转换。

二十二、时间管理

管理员可以设定对主机的控制时间（如工作时间与非工作时间、自定义时间），便于灵活管理。

二十三、跨网段管理

在实际网络应用中，经常会遇到这样的情况：某局域网中同时存在着两个或两个以上的网段（即 VLAN），各个网段间物理上联通，但相互之间不能访问，网络管理员要针对每一个网段单独进行的管理工作，重复工作量大，而且还增加了开销。针对这种情况，网络特警™上网行为管理系统特别提供了的“透明跨网段管理”这项功能，来帮助网络管理员进行跨网段的管理工作。

二十四、局域网安全管理

- 1、IP-MAC 绑定：系统支持对局域网主机进行 IP-MAC 绑定，一旦发现非法主机，即可以将其隔离网络。
- 2、嗅探主机扫描：通过使用系统附带的“反侦听技术”以及 windows 的底层分析技术，可以检测出当前对局域网危害最为严重的三大攻击工具：如局域网终结者、网络执法官、网络剪刀手等。
- 3、断开主机公网连接：系统可以断开指定主机的公网连接。
- 4、“主机强制隔离功能”：系统可以针对安装不法软件妨害局域网安全的电脑进行无条件的公网隔离功能，直至其停止使用非法软件。
- 5、“网络特警™上网行为管理系统增强性主动管理工具”：系统可以强制将局域网内的危险电脑进行紧急完全隔离，被隔离后的电脑不能访问局域网或公网，也不能被局域网或公网的任意电脑所访问，形似消失。

二十五、ARP 攻击、ARP 病毒专项检测功能

针对当前局域网内经常爆发 ARP 病毒、ARP 攻击的现状，网络特警™上网行为管理系统集成了局域网内 ARP 病毒、ARP 攻击的专项检测工具，启用此功能之后，如果局域网内有电脑遭遇 ARP 病毒和 ARP 攻击，那么网络特警™上网行为管理系统系统会自动将攻击主机进行记录，同时，网络特警™上网行为管理系统还集成了对 ARP 病毒和 ARP 攻击的自动免疫机制，会自动向局域网内发送 ARP 攻击、ARP 病毒的免疫信息，如果局域网电脑遭遇 ARP 病毒和 ARP 攻击时，网络特警™上网行为管理系统系统会自动加大免疫力度，从而可以最大程度避免局域网内电脑掉线、网络访问不正常的现象，同时也便于网管及时定位攻击源，以便

采取更进一步 的补救措施。

二十六、监控局域网内混杂模式节点、检测其他非法网管软件的功能

局域网电脑网卡处于混杂模式的节点，一般是运行某些嗅探软件或者类似的网管软件，从而对局域网的安全造成巨大的危害。因此，网络特警™上网行为管理系统提供了检测局域网混杂模式网卡的功能，从而便于网管人员迅速发现局域网危险主机，并且可以记录网卡处于混杂模式的电脑的 IP 地址和 MAC 地址；同时，网络特警™上网行为管理系统还提供了强制隔离局域网危险主机的功能，从而便于将危险主机进行防范。

二十七、检测局域网内代理服务器、禁止代理上网、禁止充当代理服务器的功能

针对局域网内部的电脑可能通过代理上网从而获取更高的上网权限，或者通过充当代理服务器为其他电脑提供代理上网功能。网络特警™上网行为管理系统提供了检测代理服务器、扫描代理服务器的功能，可以很容易扫描局域网内代理服务器、检测局域网内代理了服务器，包括扫描 HTTP 代理和扫描 SOCKS 代理，从而便于网管人员对提供代理服务的电脑进行制止和管理，防止为没有特定上网权限的电脑提供代理上网功能，避免了局域网的不当扩展，保护了网络安全、规范了网络纪律。

二十八、网络流量统计

系统提供了多种详细、图文并茂的主机流量、流速统计功能。其中包括：

- 1、日流量统计功能：系统提供了指定主机或所有主机的日流量汇总统计功能。
- 2、月流量统计功能：系统提供了指定主机或所有主机的月流量汇总统计功能。
- 3、日流速统计功能：系统提供了指定主机、指定时间内的流速趋势图。

二十九、详细日志记录

- 1、系统详细记录了所有控制信息，用户可以通过查看日志文件来确定被管理主机网络访问情况。
- 2、系统详细记录了局域网主机的 WWW 访问网址，用户可以自行查询。

三十、其他功能

除上述功能外，系统提供了许多非常实用的功能，如给局域网任意主机发送消息；可以控制局域网电脑的 USB 接口、光驱、软驱的使用；实时查看局域网主机的流速大小，并提供柱状图直观显示；记录局域网其他运行网络特警™上网行为管理系统的主机，并且正式版可以强制测试版退出等等。

网络特警™上网行为管理系统售后服务体系

大势至公司很早就意识到：为用户提供全面周到、细致入微、即时响应的技术支持和售后服务比单纯提供网管系统产品本身更为重要；同时，和其他厂家夸夸其谈如何重视服务却没有拿出具体的方略和实际的行动不同，大势至公司的售后服务条款的每一条都经得起用户的考验，六年来一直未变！

大势至（北京）软件工程有限公司主要服务内容如下：

一、产品终身使用、终身免费升级、服务终身免费为用户提供成本最低、最具性价比的网络管理

和其他网管系统设定使用年限和免费升级年限，一旦超过年限而用户没有付继续使用费和升级费，产品将不能使用或者无法升级不同或者客户需要支付服务费不同，聚生网管系统从诞生之日起就实行一次收费、终身使用、终身免费升级、享受终身免费服务的策略。从2005年开始到2011年，从早期的聚生网管系统到现在的网络特警™上网行为管理系统，我们一直奉行这种策略！我们的服务策略的首要目的就是：让国内各行业企事业单位部署总体拥有成本最低、性价比最高的网管系统，实现持续的、有效的、不断增强的网络管理，杜绝不合理的上网行为，为企业创造更大的带宽价值。

二、电话、即时通讯、远程协助软件、邮件、视频、语音等各种技术支持

自用户购买大势至（北京）软件工程有限公司后即可终身享受上述各种支持，并且这种支持也永久、全部免费，从而可以保证用户终身使用聚生网管系统、网络特警™上网行为管理系统而无后顾之忧，便于为用户创造长期的网络管理收益。

三、 对于上述手段无法解决的问题，我司派遣人员上门现场解决，直至最终解决

对于上述手段无法解决的问题，大势至（北京）软件工程有限公司将派遣专门的技术人员、研发人员亲自到客户现场帮助用户解决问题，甚至现场帮用户开发、修改网管系统，从而使得产品可以更好地适应用户的环境和用户个性化的需求，从而更快捷帮助用户实现网络管理的目的。从 2008 年以来，大势至公司派遣技术人员、研发人员累计 20 多次，赶赴江苏、浙江、上海、安徽、山东、广东、河南等地，现场培训用户使用网管系统、现场帮助用户解决使用网管系统中面临的各种问题，并深入调查用户的网络管理需求，听取用户的意见和建议，并将用户很多合理化建议集成到新版本聚生网管系统和网络特警™上网行为管理系统中，极大地提升了我公司网管系统的实用性和使用的便捷性。

四、 提供整体的网络管理解决方案而非单纯的网管系统，对网络实现全方位管理

网络管理的复杂性、多样性和不可预见性使得无论多么多么强大的网络管理系统，也不可能解决用户面临的全部网络管理问题，而只能将可能面临的网络管理问题减少到更少。为此，我们基于八年的网络管理技术的积累、实践和经验，形成了大量的网络管理有关的文档、技术和方法，涉及到网络管理的方方面面，可以协助网管人员更好地应对网络管理中出现的各种问题，更有力的保障网络的安全、稳定和畅通。同时，借助于大势至公司的研发团队和技术力量，可以随时为用户定制各种网络管理功能和扩展插件，与聚生网管系统和网络特警™上网行为管理系统相互配合，实现更全面、更精准的网络管理。

更多问题 联系我们

大势至（北京）软件工程有限公司

地址：北京海淀区中关村北大街 116 号北京大学科技园 2 号楼

邮编：100080

电话总机：010-62656060

公司传真：010-82825052

公司邮箱：service@grabsun.com

官方网址：<http://www.grabsun.com>