Neusoft东软

东软上网行为管理系统
技术白皮书

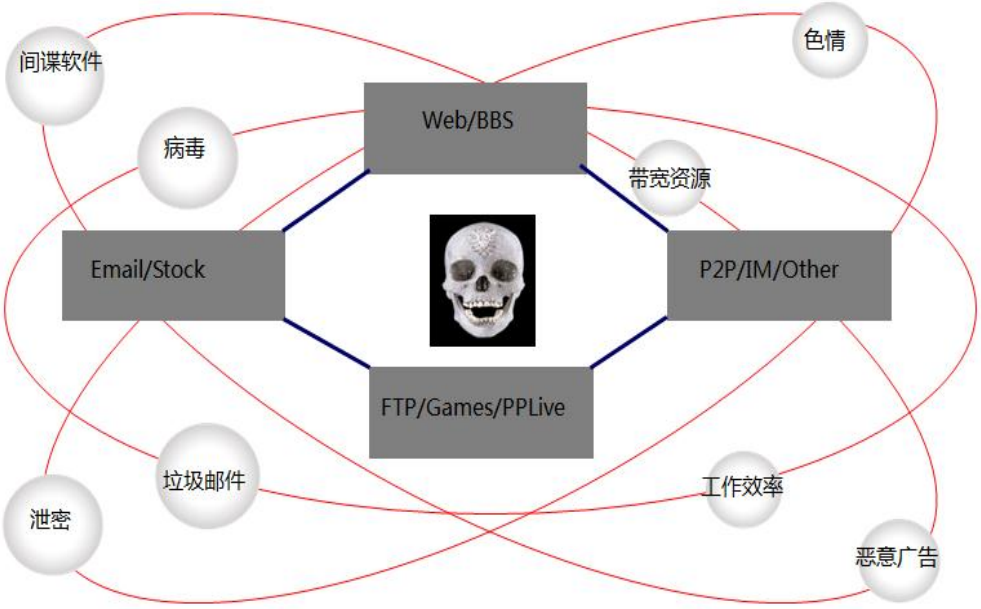
沈阳东软系统集成工程有限公司

2012

目　录

一. 前言

随着信息技术和互联网的深入发展，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时候，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也带给管理者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。互联网使用管理的缺失正让我们日益面对更多的道德、文化、法律以及使用者身心健康的问题，对互联网管理，规范上网行为，提高网络利用率等方面提出了迫切的需要。



1.1 互联网的负面影响

1.1.1 降低工作效率，增加投资成本

根据中国社会科学院社会发展研究中心2010年中国5城市互联网使用状况及影响调查报告的结果显示，被访网民使用最多的网络资源是网络新闻（65.9%），而真正用于学习和工作

的比例还不到40%。从企业角度看，员工工作效率的无法保证，也同样意味着生产成本的增加，成本的增加就意味着利润的下降，对企业造成损失。

1.1.2 机密信息外泄，组织蒙受损失

组织内部重要资料和秘密资料通过网络的Web、Email、QQ 和MSN 等途径向外散发，或被别有用心的人截获而加以利用，或是进行不当互联网访问而引起组织内部计算机感染木马病毒，加大了组织重要及秘密信息的曝光率，给组织信息安全带来隐患：

- 对于政府、事业单位以及其他公共服务单位，如果互联网管理的不够完善，将会带来极大信息安全隐患，例如经济等类型的重要的信息被通过非法渠道泄漏，此举必然会有损组织的权威及名誉，并导致组织的公信力下降；
- 对于公司企业，互联网管理的缺失会有可能导致企业重要及机密信息外泄，一旦发生企业机密信息外泄的情况，企业因此而投入了的大量人力物力将会付诸东流，此类案例在互联网广泛使用的今天是屡见不鲜的；
- 对于网吧和酒店等公共场所，由于浏览非法网页和信息，也给网吧和酒店等场所的管理者带来潜在的法律、道德等经营风险；
- 对于运营商或网络服务提供商而言，屏蔽非法言论以及不良信息是对社会应尽的义务，而且政府对此有明确要求。

1.1.3 滥用带宽资源，影响正常业务

当前的互联网存在种类众多的应用，基于前面的分析我们会发现，组织成员在使用互联网时更多的是进行娱乐活动，如网络电视、P2P 下载等；诸如此类的使用会严重消耗组织的网络带宽，正常业务通讯得不到保障，只能通过增加办公成本来增加带宽，但是网速和带宽没有得到根本的改善。

1.1.4 病毒木马肆行，安全问题凸显

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。研究发现：45%Kazaa 含恶意代码，众多的互联网访问都存在被恶意软件入侵的可能，BT、MSN 等已

成为病毒、蠕虫、间谍软件的重要传播渠道。病毒、木马及流氓软件轻者会给使用目标计算机及网络时带来一些麻烦；严重者会在组织网络中传播木马病毒，导致组织信息外泄；更严重者不仅会导致信息外泄，更能导致组织网络瘫痪，无法正常使用互联网。

1.1.5 存在不当应用，潜藏法律风险

调查发现，在日常互联网的使用中，存在以下较为普遍的现象：

- 黄赌毒是非法互联网使用的主要方面：P2P搜索、非法网站访问、非法传播不健康的信息等，最为典型的当属前一段时间的“艳照门”事件，非法的信息传播极大的恶化了互联网环境；
- 不当言论的发表，会给组织带来不必要的法律风险。很多互联网使用者在自觉与不自觉中会在互联网上发表诸如反动言论、色情、反政府、邪教等，给所在的互联网部门带来潜在的法律风险；
- 员工黑客的存在，也会给组织带来新的法律风险。

我国公安部门严格查禁利用互联网发表反动言论、色情、反政府、邪教等非法活动，详情请参考我国公安部门的相关发文。以上所述的非法互联网活动如果不加管理，将会给所在的组织带来极大的潜在法律及道德风险。

1.2 上网行为管理必要性

上网行为管理不同于传统行业的管理，无法制定简单明确的规则进行监控和管理，需要全方位深入的分析用户上网行为。一般而言，网络行为管理的难题在于：

- 网络管理者往往没有网络方面的知识，网络行为管理涉及到相当专业的技术，一般情况下管理者缺少相关的知识。
- 网络访问复杂，难以区分合理和非法的网络访问。
- 缺乏有效的跟踪分析工具，事后无法汇总、举证。
- 缺乏有效的管理控制工具，为了及时地掌握用户在网络使用中的信息，规范用户的网络行为，提高用户对互联网络资源的使用效率，就应该对用户的网络应用信息进行记录和分析，以供管理者及时发现网络应用中存在的问题，并针对这些问题提出解决的策略。

上网行为管理产品就是专门针对上网行为而设计开发的网络行为分析和管理工具，帮助管理者全面了解员工上网情况和网络使用情况，提高网络使用效率和工作效率，最大限度地避免不当的上网行为带来的潜在风险和损失。

二. 东软上网行为管理系统简介

2.1 产品概述

东软上网行为管理系统（Neusoft NetEye Internet Behavior Control：NIBC）是东软互联网管理解决方案的核心，作为完全拥有自主知识产权的上网行为管理系统，集成先进的软硬件体系构架，配以先进的行为分析，控制引擎、灵活多样的管理控制策略，实时分析网络活动，匹配管控策略，并生成丰富的统计报表。能够满足企事业单位、政府机关、金融电信、石油能源、学校教育行业等各种Internet 互联网使用单位的网络行为管理需求。

2.2 应用效果体现

- 透彻理解网络使用情况，防止互联网滥用，便于互联网管理
- 提高工作效率和网络使用效率：

通过网络使用TOP-N 排名报表、上网时间统计报表、上网时间高峰段报表，管理员能够确切的知道每个局域网用户使用网络的时间、流量、排名，并据此制定相应的管理策略，提高互联网使用效率。

- 避免单位重要资料、私密资料泄密。并可以根据保留的数据流信息，取证用户的网络访问行为。
- 避免非法网络行为带来的道德、法律风险。

三. 产品特性及优势

3.1 细致的数据库审计功能

◆ **多层业务关联审计**

东软上网行为管理系统通过应用层访问和数据库操作请求进行多层业务关联审计，实现访问者信息的完全追溯，包括：操作发生的 URL、客户端的 IP、请求报文等信息，通过多层业务关联审计更精确地定位事件发生前后所有层面的访问及操作请求，使管理人员对用户的行为一目了然，真正做到数据库操作行为可监控,违规操作可追溯。

◆ **细粒度数据库审计**

东软上网行为管理系统通过对不同数据库的 SQL 语义分析，提取出 SQL 中相关的要素（用户、SQL 操作、表、字段、视图、索引、过程、函数、包…） 实时监控来自各个层面的所有数据库活动，包括来自应用系统发起的数据库操作请求、来自数据库客户端工具的操作请求以及通过远程登录服务器后的操作请求等 通过远程命令行执行的 SQL 命令也能够被审计与分析，并对违规的操作进行记录和报警，系统不仅对数据库操作请求进行实时审计，而且还可对数据库返回结果进行完整的还原和审计，同时可以根据返回结果设置审计规则。

主机组	主机	源IP	目的IP	源端口	目的端口	数据库类型	命令	时间
后台组	主机_192.168.9.23	192.168.9.23	192.168.1.254	36390	3306	Mysql	select	2011-07-21 15:24:08
后台组	主机_192.168.9.23	192.168.9.23	192.168.1.254	36390	3306	Mysql	select	2011-07-21 15:23:33
后台组	主机_192.168.9.23	192.168.9.23	192.168.1.254	36390	3306	Mysql	select	2011-07-21 15:23:17
后台组	主机_192.168.9.80	192.168.9.80	192.168.1.254	17869	3306	Mysql	SHOW	2011-07-05 13:12:21
后台组	主机_192.168.9.80	192.168.9.80	192.168.1.254	17869	3306	Mysql	SHOW	2011-07-05 13:12:21
后台组	主机_192.168.9.80	192.168.9.80	192.168.1.254	17869	3306	Mysql	SELECT	2011-07-05 13:12:21
后台组	主机_192.168.9.80	192.168.9.80	192.168.1.254	17869	3306	Mysql	SHOW	2011-07-05 13:12:21

数据库操作命令

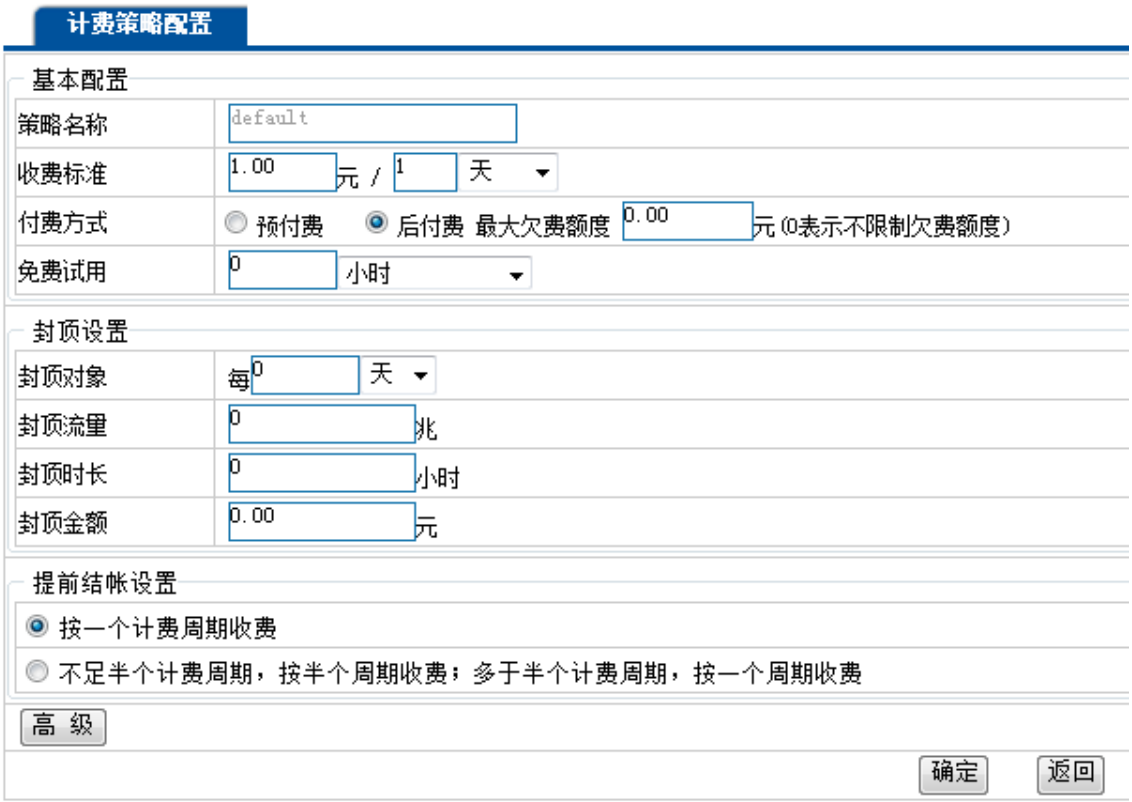
序号	时间	内容
1	2011-07-21 15:24:08	select * from conf_hos

3.2 完善的计费功能

对用户的计费是基于多种策略的，包括时间段、流量、时长优惠、流量优惠、包时包月等等。可以根据用户的需要选择基于时间、流量、包时、费用封顶等多种灵活的计费方式，并可打印完善的收费账单，或者提供与其它管理系统的接口数据以形成整体的计费管理系统。

常用的策略如下：

- 按时间段：按用户登录到用户退出登录的时间段计费；
- 按流量计费：按用户上网端口流入、流出数据量（字节数、数据包数）计费；
- 实时计费：根据用户信用度值计费；根据用户的预付款值计费；
- 优惠日计费管理：包括节假日、星期、特定日；
- 按累积时长优惠；
- 按累积流量优惠；
- 按特定时间段优惠；
- 按使用流量分段优惠；



3.3 支持单点部署与集中管理

1）单点部署方式

- 旁路接入：对现有网络应用和网络拓扑不产生任何影响，不占用网络带宽。隐藏IP模式，用户无法发现系统，更无法攻击系统。
- 网桥/路由:透明模式，不改变网络拓扑结构。路由模式节约网络设备部署费用。

2）集中管理方式

- 分布式部署、集中管理

部署方式是：在某一点的部署情况类似于单点的部署方式，但多个单点一起部署后将会给系统管理带来诸多不便，东软上网行为管理系统给出了分布部署、集中管理的解决方案：即在每一个企业分支机构按照实际需要分别部署一台东软上网行为管理系统作为上网行为管理终端，然后在企业总部部署一套管理平台，同时每一终端的管理权限交给中心机房的管理平台进行管理（管理方式可选）。管理平台可以针对所有受控终端进行管理，管理类别包括：策略下发、日志上传、日志查询等。

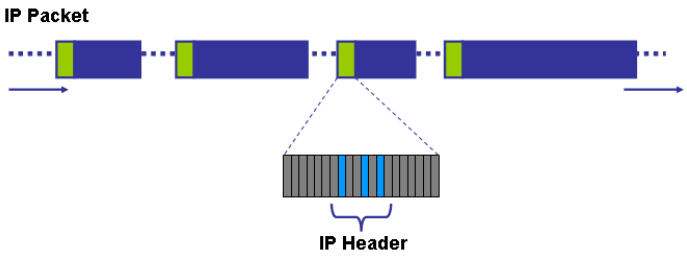
3.4 基于 WEB 的管理控制策略

- 方便易用，配备多样性的图表，所见即所得。

- 丰富的统计报表功能，避免用户二次分析数据。
- 灵活多样的管理控制策略。

3.5 DPI 与 DFI 相结合的数据分析技术

- 普通报文检测的识别方式：应用和协议识别是通过IP包头中的“五元组”即源、目标地址，协议类型，源、目的端口号信息来确定前数据包的类别；但随着网上应用类型的不断丰富，仅通过第四层端口信息已经不能够真正判断流量中的应用类型，基于开放端口、随机端口甚至采用加密方式进行传输的应用类型在目前的网络中比比皆是。端口匹配的方法虽然十分简单，但是它的局限性是十分明显的，如，目前流传比较广泛的大多数P2P应用允许用户手动选择随意的端口号来设置默认的端口号；此外，许多新出现的P2P应用倾向于使用随机的端口号，这就使得端口号不可预测；还存在一种趋势，那就是P2P应用开始使用其他熟识应用的默认端口号（例如端口号80）来伪装自己的功能端口。在这种情况下，传统的应用和协议识别逐渐显得捉襟见肘。



- DPI： 即“Deep Packet Inspection”，称为“深度包检测”。与普通的报文分析层次相比较而言的，DPI不仅分析IP包头的五元组，包括源地址、目的地址、源端口、目的端口以及协议类型，而且，还增加了应用层分析，识别各种应用及其内容。
- DFI：即“Deep/Dynamic Flow Inspection”深度/动态流检测技术，DFI技术是一种较新的应用流量分析技术，与DPI进行应用层的载荷（payload）分析匹配不同，DFI采用的是一种基于流量行为的应用识别技术，即不同的应用类型体现在会话连接或数据流上的状态各有不同。它通过应用流的平均速率、流持续时间、字节数、包长等流特征信息来实现应用流量的识别。即不同的应用类型体现在会话连接或数据流上的状态各有不同。例如，网上IP语音流量体现在流状态上的特征就非常明显：RTP流的包长相对固定，一般在

130～220byte，连接速率较低，为20～84kbit/s，同时会话持续时间也相对较长；而基于P2P下载应用的流量模型的特点为平均包长都在450byte以上、下载时间长、连接速率高、首选传输层协议为TCP等。DFI技术正是基于这一系列流量的行为特征，建立流量特征模型，通过分析会话连接流的包长、连接速率、传输字节量、包与包之间的间隔等信息来与流量模型对比，从而实现鉴别应用类型。

- 东软上网行为管理系统：鉴于DPI在应用区分、识别精度、功能扩展等方面优势明显，而DFI在对新应用和加密协议的识别方面有一定的优势。东软上网行为管理系统采用了以DPI分析技术为主，辅助于传统普通报文分析和DFI技术来处理分析加密应用协议的方式来综合分析数据包。即综合分析应用层特征值和应用协议行为：UDP/TCP 端口、端口范围和端口列表，IP 地址、地址范围、子网或主机列表，MAC地址，VLAN标签、MPLS 标签、IP PRECEDENCE、MPLS EXP，传输方向等，以此来达到精确分析应用和协议的目的。

3.6 准确完善的 URL 分类库

系统中集成了默认的 URL 分类库，这些分类库是根据中国的当前情况而进行了合理的采集及分类，符合我国用户的网络使用环境的需求。目前 URL 分类库是由东软公司组织专门的团队进行人工分类的，并参照国内专业机构所提供的专业数据，分类结果较为准确，所涵盖的 URL 地址类型也较为全面，基本覆盖了在国内用户中有一定访问量的 URL 地址。

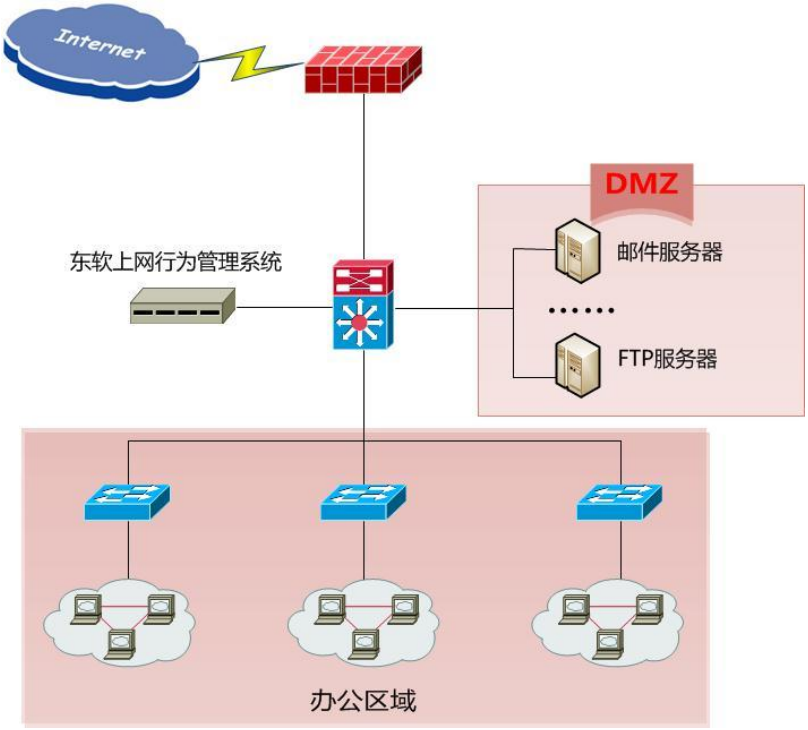
3.7 定期更新 URL 库及应用库

为保证URL分类库的准确性及实时性，系统会定期更新URL分类库；由于系统是基于应用对数据进行分析的，因此在当前诸如MSN、QQ等即时聊天软件，钱龙、大智慧等股票软件以及P2P下载软件等等的应用特征码不断更新的情况下，也会定期更新系统的应用协议库，以保证对所有网络应用的准确识别。

四. 产品部署

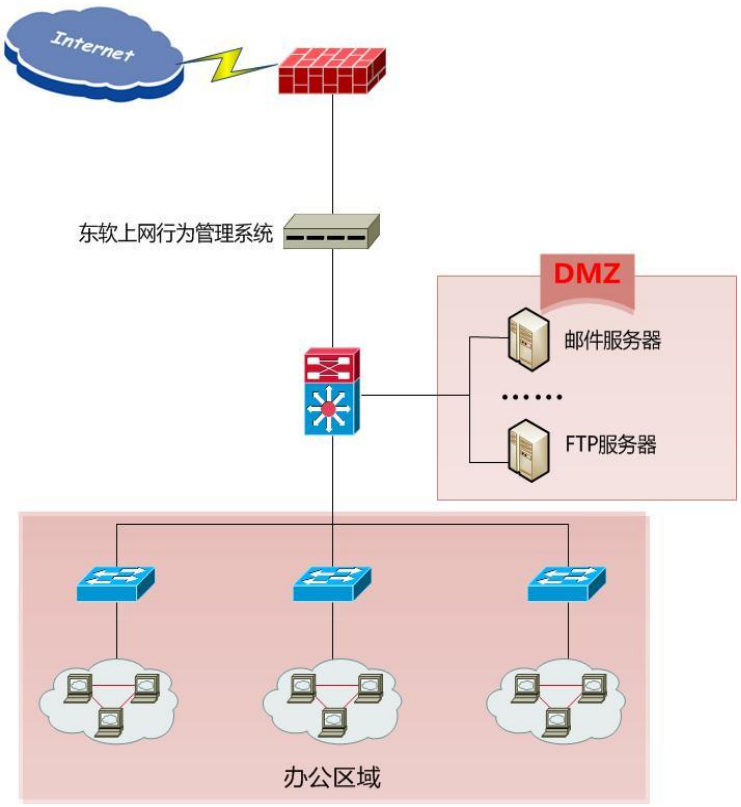
4.1 旁路部署模式

东软上网行为管理系统可以采用多种方式灵活地部署，通过分析处理流入和流出的数据包，有效地实现对网络数据的监控。下图为旁路接入方式的部署结构：



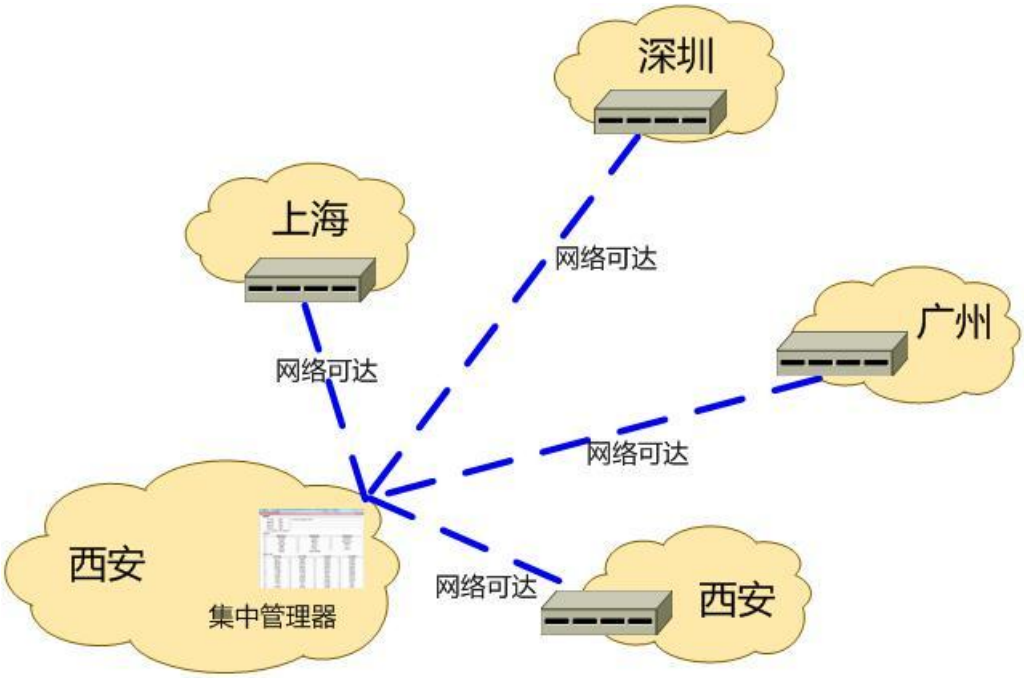
4.2 路由或网桥部署模式

东软上网行为管理系统支持串联的部署方式，包括路由和透明网桥模式，如下图所示：



4.3 集中管理的部署模式

在支持单点部署的同时，东软上网行为管理系统还支持分布式部署、集中管理的模式，大大方便了存在多个分支机构的集群用户的管理。


深圳
上海
网络可达
网络可达
广州
网络可达
西安
集中管理器
网络可达
西安