LanSecS®
莱 恩 赛 克

LanSecS 内网安全管理系统 V7.0

技术白皮书

北京圣博润高新技术股份有限公司
2013 年 11 月

版权声明

信息更新

本文档仅用于为渠道代理商或最终用户提供信息，并且随时可由圣博润公司更改或撤回。

免责条款

根据适用法律的许可范围，圣博润公司按“原样”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性或无侵害性。在任何情况下，圣博润公司都不会对最终用户或任何第三方因使用本文档造成的任何直接或间接损失或损坏负责，即使圣博润公司明确得知这些损失或损坏，这些损坏包括（但不限于）利润损失、业务中断、信誉或数据丢失。

目录

1. 产品简介

随着互联网技术飞速发展，单位网络结构日趋复杂，总部对部门、分支机构的管理比较困难。在网络中各个节点均可能造成病毒传播、非法接入和违规操作等问题，内网安全风险日益凸显；各节点随意连接互联网，工作时间 P2P 下载占用较大的带宽资源，随意接入一些不良网站，造成网络中大量木马、病毒的传播，带来安全隐患；内部 ARP 欺骗现象严重，网络故障无法准确定位，单位涉密信息被非法泄漏等，都严重影响了单位业务的发展。

虽然越来越多的单位开始重视网络建设并有了很大的发展，但网络自身仍然比较脆弱，安全性不高。在日常管理中存在着不少问题，例如：难以监控外来计算机接入内网、IP 地址使用存在一定混乱、各类网络基础信息搜集不全、外围设备使用控制困难、操作系统补丁问题、文件拷出与打印等难以监控管理。

分析表明，单位的网络信息安全建设是一项复杂的系统工程。科学的建立内、外网是网络安全的基础，应用软、硬件技术是保证网络安全的手段，而建立起单位信息安全管理制度则是网络安全的保证。为了建立起完善的内网安全管理机制，保护政府及企业内部网络的安全，北京圣博润高新技术股份有限公司（以下简称圣博润）推出了专门用于政府和企业终端安全管理的 LanSecS®内网安全管理系统。

LanSecS®内网安全管理系统通过对计算机准入控制、计算机安全加固、计算机运行维护、计算机安全审计、移动存储介质注册等多个方面的综合管理，为政府和企业用户打造一个安全、可信、规范、健康的内网环境。LanSecS®内网安全管理系统 V7.0 是圣博润公司的一个里程碑式的、战略性的产品版本，该版本通过系统架构的优化调整和用户需求的持续跟踪，使得产品性能显著提升、产品功能进一步丰富。借助 LanSecS®内网安全管理系统 v7.0 的发布，圣博润公司更加明确地宣告了其专注于内网安全管理领域的决心。LanSecS®内网安全管理系统可为用户解决如下一系列的内网安全管理问题：

- 确保入网终端符合要求
- 全面监测终端健康状况
- 保证终端信息安全可控
- 动态监测内网安全态势
- 快速定位解决终端故障
- 规范企业员工网络行为
- 统一内网用户身份管理
- 杜绝移动存储介质滥用
- 提高和实现软件正版化

在为用户提供终端安全保护手段的同时，LanSecS®内网安全管理系统更加强调为用户提供便利的终端运维管理手段。集中式、人性化的终端管理能力是 LanSecS®内网安全管理系统的特色之一，也是圣博润公司一直以来的努力方向。

2. 产品构架

图 1 LanSecS®内网安全管理系统架构

LanSecS®内网安全管理系统在架构设计上采用了三层管理结构：终端监控引擎、总控中心、管理控制台。

2.1. 终端监控引擎

终端监控引擎以服务的形式运行于终端计算机上，是终端计算机管理的核心和基础部件，用于对被管理终端计算机的安全加固、运行维护和监测审计等管理职能。终端监控引擎可以部署在所有 Windows 系列操作系统上，包括 Windows 2000、Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008、Windows 7、windows8、windows Server 2012。

终端监控引擎的设计充分考虑了稳定性、安全性和兼容性要求。终端监控引擎可防止恶意停止，并全面兼容防病毒软件、防火墙软件、设计开发软件、业务软件、办公软件。

2.2. 总控中心

总控中心用于计算机的集中管理，为终端监控引擎和管理控制台提供一系列的管理服务。由注册管理服务、认证管理服务、策略管理服务、审计管理服务、补丁/软件分发服务等组成。视内网规模和性能要求，这些服务可分别部署在不同的硬件平台上，也可部署在同一个硬件平台上。

- 策略管理服务：负责终端计算机策略的配置和更新。
- 审计管理服务：负责接收终端监控引擎发送的审计信息与事件报警，并存储到数据库中。
- 接入认证服务：负责对接入内网的终端计算机身份和健康状况进行认证。
- 文件备份服务：提供集中的文件备份。文件备份服务支持用户身份认证。
- 补丁分发服务：提供补丁文件和软件的下载服务，支持 FTP 和 HTTP 两种方式。
- 时间同步服务：为终端计算机提供统一的标准时间服务，便于终端计算机的时间管理。
- 网络管理服务：提供网络拓扑扫描服务，可绘制网络的链路层拓扑。
- 分级管理服务：提供分级部署环境下的分级管理。
- 事件订阅服务：接受报警监控程序的事件订阅，根据订阅条件向报警监控程序发送符合要求的报警事件，可向多个报警监控程序同时提供服务。
- 健康检测服务：用于总控中心自身各服务的运行状态监控。

2.3. 管理控制台

管理控制台是系统管理人员提供系统管理入口。采用了 B/S 方式进行系统管理，通过管理控制台可以完成系统管理的全部操作。

2.4. 系统数据库

系统数据库用于存储策略、信息和事件，全面支持目前主流数据库，包括：SQL Server、MySQL、Oracle、IBM DB2、PostGreSQL、Gbase。

总控中心与数据库之间采用数据库访问中间件和网络缓存技术实现高速数据访问。通过数据库访问中间件和网络缓存，可以大大降低数据库的访问压力，提高数据的存储和访问能力。

终端监控引擎和总控中心之间采用 ICE 网络通讯中间件进行相互通讯。通过 SSL 协议对通信过程进行认证和加密，增强组件间通信的安全性。

三层管理结构大大提高了系统设计开发、安装部署和运行维护的灵活性、便利性和扩展性。

3. 产品功能

3.1. 终端运维管理

内网的可靠运行是业务系统可靠运行的保障。内网的可靠运行依赖于网络设备、服务器和个人终端计算机的安全运行，任何一个环节出现故障，都可能对内网的可靠性产生不可估

量的冲击。

内网中主要设备是终端计算机，终端计算机的安全运行与管理对整个内网安全有至关重要的作用。系统对终端计算机的管理采取了两种不同的安全措施：系统运行管理和系统监测。

系统运行管理方面主要包括补丁管理、主机资产管理、主机防病毒管理、系统日志管理、时间同步、消息分发及文件备份，通过系统运行管理确保终端主机以最安全的状态运行，有效地减少病毒爆发和木马泛滥带来的内网安全隐患，减少终端计算机被入侵的可能性。

系统监测方面主要包括主机性能、网络流量、健康状态、设备入网、时间同步与安全态势分析等。通过系统检测可以让管理员及时了解整个网络内终端主机的状态，针对存在的安全隐患及时采取有效措施，更好地保证内网的可靠性。

具体功能如下：

表 1 运维管理功能列表

模块名称	功能描述
设备入网监测	提供对内网设备入网的实时发现、状态报告和阻断等功能。通过实时设备扫描可发现所有当前在线计算机，通过总控中心的计算机注册信息的同步，可区分合法设备和非法设备。对于非法设备，可采取入网阻断措施。
防病毒软件管理	可支持多种防病毒软件检查方式，提供防病毒软件信息收集和状态监测功能，信息收集包括防病毒软件名称、软件版本、病毒库版本等。
网络流量监测	对终端计算机的网络通讯流量的审计、控制和统计。
健康监测	对终端计算机的健康状况进行监测，并为终端计算机用户提供手动评估计算机健康状况的手段。
文档安全	可支持将文件备份到指定的备份服务器和文件粉碎。
时钟同步	以安装有时间服务的计算机硬件时间为时间源，为内网终端计算机提供标准的 Internet 时间服务。
性能监测	通过为 CPU、内存、硬盘设定阈值，实现对终端计算机的 CPU、内存和磁盘使用情况的动态监测，可进行连通性监控，实时监测主要系统的网络或网络服务端口，保证系统正常运行。
系统日志管理	提供对终端计算机本地日志收集、日志转储、日志清理的功能
远程协助	提供终端计算机的远程监控和远程桌面接管的功能。
资产管理	提供计算机资产自动收集、资产注册登记、资产变更管理、设备维修管理、资产查询与统计等管理。

补丁管理	可以实现 Windows 平台下的补丁审批、分发和补丁修复状态统计，管理、分发和自动安装 Windows 系列操作系统补丁和微软应用程序补丁。
消息分发	提供对内网全部或者部分终端计算机的消息通知功能。
软件分发	提供对内网全部或者部分终端计算机的软件分发管理。由分发管理工具、文件下载服务器和终端监控引擎等组件组成。

3.2. 终端安全加固

终端主机的安全运行是整个网络的基础，而终端主机运行参数、运行策略的稳定又是终端主机安全运行的保障，系统的具体加固措施包括如下方面：

表 2 终端安全加固功能列表

模块名称	功能描述
终端安全配置	管理终端计算机的本地安全策略、对本地系统环境进行安全设置管理，从而实现主机运行安全策略的最优化，确保对终端主机的安全管理
终端防火墙	系统内置防火墙是基于 NDIS 的桌面防火墙，对终端计算机的访问目标进行限定，对终端计算机的网络访问进行控制。具有基于优先级的网络访问控制能力、提供网络访问审计能力、支持策略模板
网络接入认证	系统提供了“主动防护”和“动态监控”相结合的计算机准入控制机制。可通过内部 DNS 服务器(Windows2003/2008)加壳和系统内置认证网关保证接入内网的主机合法，用户身份可查可控。
网络通讯认证	通过设置 IP 筛选器、筛选器操作、身份验证方法、隧道设置、连接类型，实现对内网中两台终端计算机之间的通讯进行管理
移动存储介质管理	根据移动存储介质的不同特点和使用要求将移动存储介质的分为五种管理模式：未授权移动存储介质、加密移动存储介质、多分区 U 盘、专用安全 U 盘、特权移动存储介质。通过对介质的使用授权控制和文件操作审计保证数据完全。
网络参数配置	对终端计算机的网络相关参数的配置和变更监控管理，包括参数绑定、参数变更监控、ARP 攻击防护与 IP 地址保护，具有支持多个网络参数的统一配置管理、支持多个同类参数的绑定、支持 IP 地址范

	围控制等特点

3.3. 终端安全审计

任何政府部门和企业单位，均拥有自己的机密信息。这些机密信息，如果没有良好的技术防护手段，很容易发生侵害政府和企业利益的信息泄露事件。政府和企业面临的信息泄露威胁有两种：被动信息泄露和主动信息泄露。

被动信息泄露：由于人员缺乏信息保密意识，常常由于专业知识不熟悉或者工作疏忽而造成泄密。如有些人由于不知道计算机的电磁波辐射会泄露秘密信息，计算机工作时未采取任何措施，因而给他人提供窃密的机会；有些人由于不知道计算机软盘上的剩磁可以提取还原，将曾经存贮过秘密信息的软盘交流出去，因而造成泄密；有些人因事离机时没有及时关机，或者采取屏幕保护加密措施，使各种输入、输出信息暴露在界面上；有些人对自己使用的计算机终端缺乏防护意识，如没有及时升级病毒库和更新系统补丁，导致病毒和木马的入侵，在不知不觉中泄露了机密信息。

主动信息泄露：这种情况是由于内部人员出于个人利益或者发泄不满情绪，有意识的收集和窃取机密信息。由于电子信息文档不像统文档那样直观，极易被复制，且不会留下痕迹，所以窃取秘密也非常容易。电子计算机操作人员徇私枉法，受亲友或朋友委托，通过计算机查询有关案情，就可以向有关人员泄露案情。计算机操作人员被收买，泄露计算机系统软件保密措施，口令或密钥，就会使不法分子打入计算机网络，窃取信息系统、数据库内的重要秘密。

对于政府部门和企业来说，计算机终端作为信息处理的工具，在其上存储、传输和处理的信息的安全性保护相当重要。任何一个环节的疏漏均可导致信息的丢失。因此，必须加强对信息的监控和审计管理。LanSecS®内网安全管理系统提供了设备输出监控、违规外联监控、共享监控、打印监控、文件监控、账户监控、进程监控、服务监控、软件安装监控、注册表监控和网络行为审计等一系列信息监控与审计功能，为政府和企业的信息保密与信息防护提供了有力的技术手段和工具。

表 3 终端安全审计功能列表

模块名称	功能描述
进程监控	对本地计算机运行程序通过黑名单、白名单和红名单方式进行管理，包括运行控制、运行保护、运行统计与进程别名管理
服务监控	对本地计算机上所运行服务进行管理，控制本地服务的运行状况。通过黑名单、白名单和红名单方式管理
打印监控	对终端计算机的打印操作进行监控与管理。全面监控本地打印、共享打印和虚拟打印。还支持对打印文档的扩展名进行过滤。
文件监控	对文件的四种操作行为：创建、删除、重命名、修改进行审计；对文件内容进行关键字审计；对符合内容检查的文件进行备份。
注册表监控	对终端计算机本地注册表进行访问监控和自动恢复保护（暂不支持

	64bit 操作系统）
共享监控	能够监控终端计算机的系统默认共享、用户文件夹共享。共享文件夹的操作权限情况进行监控，避免内网用户通过共享的途径获取到机密信息并导致外泄
设备监控	对硬件设备的使用进行监控。采取黑名单和白名单的控制方式，可区分普通光驱和刻录机
账户监控	对本地计算机账户的相关安全参数进行配置，对账户变更进行监控和审计
网络行为审计	网络行为审计提供对终端计算机的网络访问的监控与审计。包括 HTTP 访问、SMTP/POP3 邮件收发、WEB 邮件收发等。系统提供基于规则的访问控制手段。
违规外联监控	实时监测和阻断终端计算机的 MODEM 拨号、ADSL 拨号、多网卡上网、非法外联等行为，实现对终端计算机连接互联网或者其它网络行为的严格控制
软件安装监控	对终端计算机上的软件安装行为进行监控与控制，还可支持黑名单、红名单两种检查方式

3.4. 网络准入控制

系统提供了“主动防护”和“动态监控”相结合的计算机准入控制机制。“主动防护”是指：在计算机接入网络之前，首先验证其身份信息和安全状态，以决定是否允许其接入网络。这与以往的安全思路“先接入网络，再验证其身份”相比，极大地提高了网络的安全性。

“动态监控”是指：当计算机通过验证并接入网络后，并非该计算机就可以在接入期间不受控制地访问网络资源。系统还会动态地对接入计算机的身份和安全状态进行跟踪和检测，一旦发现身份信息和安全状态有变，即刻对其重新隔离。

主机健康检查：对接入内网的计算机的安全状况进行检查

接入认证：对主机进行身份认证，系统支持用户名/口令、PKI 数字证书以及设备特征标识三种身份信息的认证方式。

主机隔离与修复：根据策略将未通过认证的主机隔离到修复区/工作区/访客区。

主机状态动态检测：对接入网络的计算机进行动态监测，监测的内容包括身份确认、安全状态确认等。

IP 通讯控制：网内主机之间的通讯采用 PKI 数字证书标识双方的身份，并同时对通讯数据进行加密。

3.5. 移动存储管理

USB 移动存储介质是目前使用最为广泛的数据交换手段。也正因为 USB 移动存储介质使用的广泛性，为政府和企业内网信息的安全防护带来了很大的安全隐患，如何对其进行有效的管理，成为政府、企业和信息安全产品提供商需要共同面对的问题。系统通过对移动存储介质实施注册管理，有效避免了移动存储介质的滥用，以此提高政府和企业内网信息的安全性。

移动存储介质注册管理是指将移动存储介质进行特殊处理后，在移动存储介质无法被直接访问的区域写入该移动存储介质相对应的注册信息，注册信息包括两种类型：**标记信息：**用于标明该移动存储介质的所有者、联系方式、管理者、所属部门等。**访问控制信息：**当该移动存储介质插入计算机时，依靠访问控制信息决定是否允许在计算机上使用。

根据用户管理需求的不同，系统将移动存储介质的管理分为五种管理模式：未授权移动存储介质、安全 U 盘、多分区 U 盘、专用安全 U 盘、特权 U 盘。注册介质的授权使用范围包括全局、部门与主机三个选项。注册介质的授权操作权限包括只读、读写与禁用、只写四种工作模式。

系统通过专用工具对各种存储介质进行注册管理，系统自带 U 盘资源管理器，实现对注册移动存储介质的访问与文件操作，有效地保证了移动存储介质管理的安全性。

系统采用了文件操作动态监控和审计的技术思路。当有文件在加密移动存储介质和本地磁盘进行拷贝时，系统将自动记录文件操作行为，包括访问、创建、删除、修改等。

表 4 终移动存储介质管理功能列表

类型	说明
未授权移动存储介质	所有未在系统中进行注册管理的移动存储介质。系统默认将自动禁止其在装有终端监控引擎的计算机上使用
安全 U 盘	经过系统加密格式化并注册的移动存储介质
多分区 U 盘	经过系统格式化为多个分区并注册的 U 盘，包括启动区、交换区、加密区、日志区，用户的访问操作权限可细化到分区
专用安全 U 盘	与系统配套提供的专用 U 盘，可格式化为多个分区，自带 COS 操作系统
特权 U 盘	经系统注册并打印特权标签的移动存储介质，尤其适用于各种数码产品存储卡

4. 产品性能

4.1. 终端引擎性能

终端监控引擎设计时充分考虑了其可能对桌面计算机造成的性能影响，通过多次优化，

形成了现在的终端监控引擎架构。该架构保证了终端监控引擎在稳定可靠运行的前提下，仍能保持极少的静态工作模式系统资源占用。

经过严格的第三方测试，以及大量用户的实际使用证明，终端监控引擎在静态工作模式下，对系统资源的占用几乎可以达到零消耗。静态工作模式下，CPU 的占用率低于 1%，内存占用低于 10M，网络带宽占用低于 0.2K/s/客户端。

4.2. 总控中心性能

LanSecS®内网安全管理系总控中心采用了分层设计理念，系统架构设计时采用了分布式负载均衡技术和动态性能扩展技术，路由与定位服务、业务服务、数据库服务均支持多个服务镜像，从而能有效分散终端计算机连接请求，实现负载均衡。同时，在系统运行过程中，可以根据业务需要随时增加路由与定位服务、业务服务和数据库服务镜像，以达到动态性能扩展的目的。系统可以在一个总控中心单元管理 2 万台终端计算机。

4.3. 自身安全性

LanSecS 系统设计之初便对其自身安全性做了充分的考虑和技术处理，使得 LanSecS 系统的安全性得到了有效的保障。在自身安全性方面，主要考虑了如下几个安全问题：

- 总控中心安全性：系统通过采用最小服务原则、系统管理控制、代理访问认证等几个措施确保总控中心的安全运行。
- 终端监控引擎安全性：系统通过采用监控进程隐藏技术、本地文件访问保护、多入口恢复技术及监控引擎完整性校验技术等确保终端监控引擎的安全运行。
- 数据库安全性：系统通过采用数据库访问控制、数据加密与数据备份等措施确保数据库的安全运行。
- 策略安全性：系统通过策略订单生成控制、加密策略传递与存储、策略完整性校验等措施确保策略的安全性。
- 通讯安全性：系统通过采用加密传输、身份认证、本地安全存储等措施确保终端监控引擎与总控中心之间的通讯的安全运行。

4.4. 产品性能指标

LanSecS®内网安全管理系统主要性能指标如下：

- 总控中心最大并发连接数：3000；
- 总控中心最大可管理注册主机数量：20000 台；
- 总控中心网络带宽占用：100K/1000 客户端；
- 终端监控引擎 CPU 占用（静态模式）：＜1%；

- 终端监控引擎内存占用（静态模式）：8M。

5. 产品部署

5.1. 产品形态

LanSecS®内网安全管理系统提供网络版和单机版两种产品版本。网络版适用于对联网的内网计算机进行统一的安全管理，而单机版则适用于对未接入内网的独立计算机进行安全管理。用户可以根据自己的实际情况选择部署和使用两种版本中的任何一种。

- 网络版：网络版产品可以提供最大的管理灵活性和方便性。通过计算机的集中管理，实现内网策略的统一和报警事件的集中管理和响应。
- 单机版：单机版产品可以对孤立的计算机进行单独管理。策略的配置和事件的管理均在本地计算机实现。

5.2. 部署方式

LanSecS®内网安全管理系统提供本地和分级两种产品部署方式。用户可以根据网络的实际环境选择合适的部署方式进行产品的部署实施。

5.2.1. 本地部署

本地部署是本系统最常见的部署方式。适用于计算机终端数量不多（例如，小于 10000 台）并希望对所有终端计算机进行集中管理的用户环境。在该部署方式下，所有的计算机终端注册到同一个总控中心。本地部署的优点是可以在一个系统管理中心监控到内网中所有计算机的活动状况。其部署示意图如下：

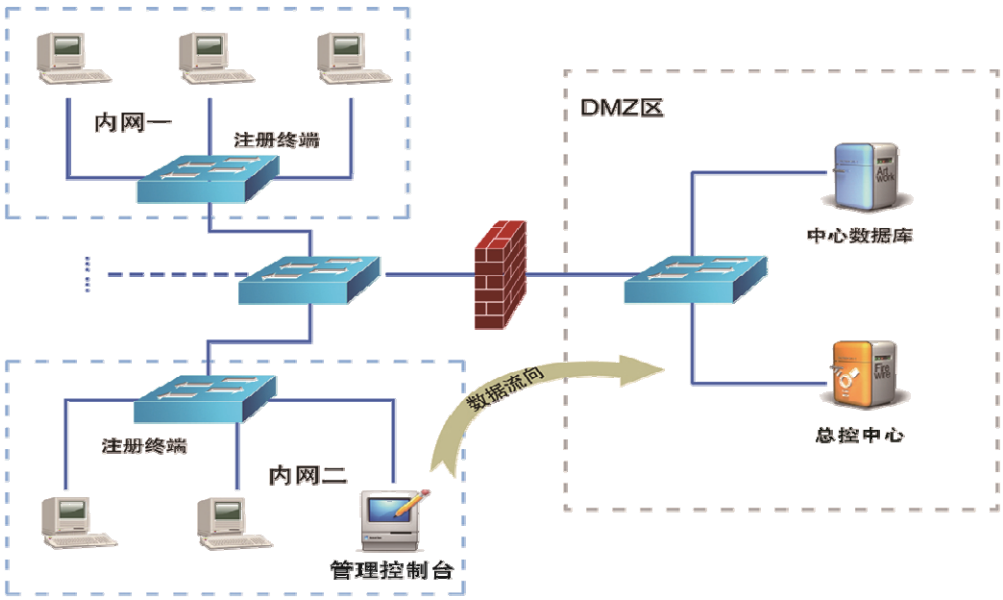

图 2 本地部署示意图

5.2.2. 分级部署

分级部署是指在按照地域或者部门的不同，在内网中安装多个总控中心，不同地域或者部门的计算机分别注册到不同的总控中心。总控中心之间通过分级注册，形成上下级关联关系。

上下级关联关系确认后，可以对整个系统实行分级管理。上级可以对下级分发终端监控引擎安全策略，上级也可要求下级将安全事件上报到上级总控中心。从而实现上级对下级的管理。

分级部署方式的优点是，可以将实际的日常运维管理权限分散到不同的部门或区域，但上级仍然可以保证对下级的管理能力。另外，通过分级部署，可以无限的增大计算机管理数量。例如，可以通过分级部署管理多达几十万台的计算机。分级部署示意图如下：

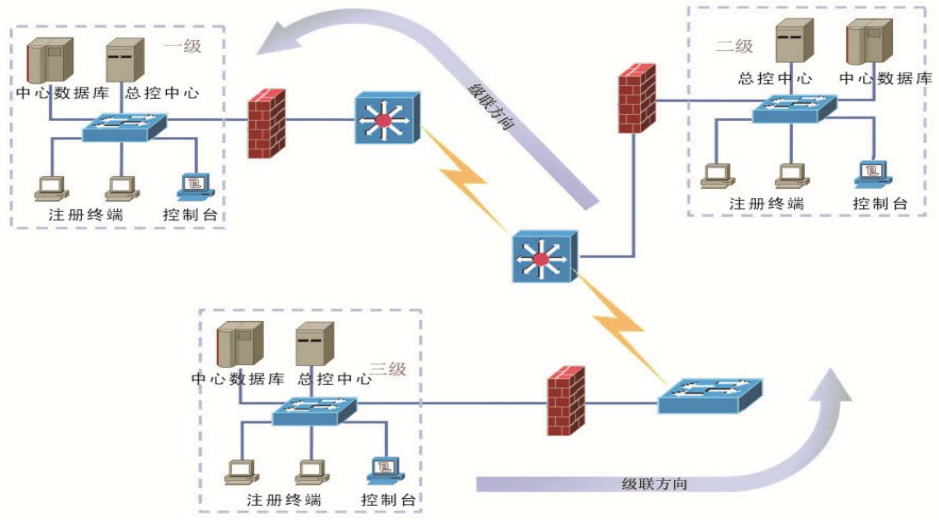

图 3 分级部署示意图

6. 产品特色

6.1. 先进的系统架构和稳定的系统性能

- 系统采用了先进的分层设计思想，将总控中心分为数据层、业务层、网络访问层三个逻辑层，不同层之间通过中间件无缝组合在一起。使得系统的性能得到极大的提高。另外，系统还支持分级、分权管理。与国内同类产品相比，系统架构具有先进性。
- 系统采用了稳定的第三方技术，成熟的中间件和国际标准的通讯协议确保了稳定的系统性能。如：终端监控引擎与总控中心、管理控制台与总控中心之间的通讯采用了 ICE 通讯中间件；总控中心对数据库的访问采用了 Hibernate 中间件；加密通讯采用了标准的 SSL 协议。这些中间件的成熟性和稳定性得到了业内的公认。此种设

计理念，与国内其他同类产品采取的自行设计通讯接口的设计理念相比，技术更加稳定可靠，为保障系统的稳定性打下了良好的基础。

- LanSecS®内网安全管理系统的终端监控引擎具有良好的系统和软件兼容性，可尽最大限度地保护用户的资产投资。主要体现在如下几个方面：
  - 全面兼容 Windows 系列操作系统平台；
  - 全面兼容国内外主流安全软件，如防病毒软件、防火墙软件；
  - 全面兼容各类设计软件、开发软件、业务软件、办公软件；
  - 安全代理通讯不受 Windows 自带个人防火墙的限制。
- 系统设计和开发时采取了多套方案以保障系统运行的可靠性。主要体现在如下几个方面：
  - 系统具备完备的备份和恢复功能，可以对注册和运行数据进行人工或者自动的备份，数据的恢复可在数分钟内完成；
  - 系统采用了冗余设计原则，对于路由器服务和重要的业务服务，可以部署多个镜像服务。当一个服务器由于故障停止工作时，镜像服务仍可提供有效的服务支持；
  - 系统还采用了延后处理机制，在业务服务（如事件管理服务）暂时不可用时，可以将关键数据保存在本地，待业务服务恢复后，重新将数据上传至总控中心；
  - 系统还支持第三方负载均衡和冗余备份方案，可以对数据库进行负载均衡和冗余备份处理。

6.2. 分布负载均衡和动态性能扩展

- 强大的定位和路由服务可智能地分配代理连接到不同总控中心的服务组件，可有效平衡总控中心的负载；
- 任何总控中心服务组件均可以在同一台计算机或不同计算机上创建多个服务镜像，可显著提高系统的性能；
- 当总控中心负载过高时，可随时添加任意一台新的计算机到总控中心服务集群中，快速缓解总控中心负载压力。

6.3. 全面主流数据库支持

- 系统支持目前大多数的主流数据库系统，可使用户节约项目采购资金。产品支持的

数据库包括：SQL Server、MySql、Oracle、 IBM DB2、PostGre、SQLGBase；

- 您可以采用已经采购的数据库系统作为数据支撑平台，最大限度地保护您的投资价值；
- 选择开源数据库可让您节省采购成本；
- 选择国产数据库可让您的涉密应用更加安全。

6.4. 全面支持 Windows 8/server2012 系统

- 在计算机桌面安全管理领域，业内率先支持Windows 8/windows server2012操作系统，由此产品已全面覆盖Windows 系列操作系统；
- 您可以放心升级您的操作系统到Windows 8，在体验Windows 8 便利与友好的同时，不必担心您的桌面管理系统无法升级。

6.5. 统一的身份管理

- 安全策略账户、Radius 认证账户和文件备份账户的统一管理，可大大减轻管理员维护系统账户的压力；
- 唯一的账户管理入口，可让账户信息的变更实时同步到所有相关服务组件；
- 账户同步接口可将 Windows 域账户、应用系统 LDAP 账户方便地同步到系统中，省去管理员一一创建账户的麻烦。

6.6. 丰富的策略管理模式

- 网络策略可让计算机在多个不同的网络之间移动，且其安全策略随网络位置的变更而动态改变。科学的策略设置，让计算机无论处在何种网络中，都能按照最合适的策略运行，以适应不同网络的管理要求；
- 账户策略可在多人使用同一台计算机时，计算机的安全策略截然不同，也可让同一用户在不同的计算机上保持一致的安全策略，确保计算机中存储的重要信息和关键数据免遭破坏；
- 主机策略、账户策略和网络策略的随意组合，可满足随时变化的策略管理需求。

6.7. 灵活多样的部署策略

- 安装与卸载策略可让代理的安装与卸载控制更加灵活，最大限度满足系统部署要求；
- 智能部门匹配策略可让计算机自动分组到预先设定的组织结构中；

- 代理安装和卸载的审批管理让系统部署过程更加人性化。

6.8. 强大的终端安全态势分析

- 安全态势分析可让计算机终端的安全变化趋势一目了然，为计算机安全策略的动态调整提供科学的决策支持，也为内网的安全建设提供科学、客观的参考数据；
- 不仅可对单台计算机，还可对一个部门或整个单位的综合安全状况绘制态势分析图，提前掌握内网安全趋势，达到持续跟踪和改善内网整体安全状况的目的。

6.9. 尽善尽美的分级管理模型

- 系统的分级管理模型课支持任意多级管理，支持级间策略分发和数据同步，以及分级服务器的运维监测；
- 细粒度的分级策略，任意策略项均可强制执行、建议执行或者忽略；
- 分级数据同步支持注册数据、安全事件、运维数据等几乎所有下级信息的同步；
- 支持分级拓扑展示，通过服务器运维监控可实时监测下级服务器的运行状况。

6.10. 更具人性化的系统管理

- 全新的 B/S 管理结构，让系统管理更容易；
- 丰富的内置策略模板和数据模板让系统配置过程更加简单和轻松；
- 启发式操作向导让您的策略、软件和消息的分发过程更加便捷；
- 全面的查询、统计和分析报告为您提供更加完整和科学的数据支持。

7. 产品规范

LanSecS®内网安全管理系统的设计参考了如下国家标准规范：

- BMB17-2006：《涉及国家秘密的信息系统分级保护技术要求》
- BMB20-2007：《涉及国家秘密的信息系统分级保护管理规范》
- BMB22-2007：《涉及国家秘密的计算机信息系统分级保护测评指南》
- GB/T22239-2008：《信息系统安全等级保护基本要求》
- GBT 22240-2008：《信息系统安全等级保护定级指南》
- GBT 22241-2008：《信息系统安全等级保护实施指南》

8. 资质和荣誉

8.1. 产品资质

- 国家保密局《涉密信息系统产品检测证书》
- 公安部《计算机信息系统安全专用产品销售许可证》
- 中国信息安全测评中心《国家信息安全测评信息技术产品安全测评证书》
- 自主创新产品认证证书

8.2. 所获荣誉

- 2005 年中国信息安全值得信赖内网安全品牌
- 2006 年中国信息安全市场优秀内网安全产品推荐品牌奖
- 2006 年计算机网络系统信息防护解决方案优秀奖
- 2007 年最具价值的内网安全产品奖
- 2008 年度内网安全最佳产品奖
- “中国计算机用户协会 25 周年”内网安全产品信赖品牌
- 2009 年度中国信息安全值得信赖品牌奖
- 奥运政务网络和信息安全优秀服务企业

北京圣博润高新技术股份有限公司

北京市海淀区西土城路 8 号科研楼十层

邮编：100088

电话：010-82138088

传真：010-82137982

技术支持热线：800-810-2332

网址：www.sbr-info.com