

# 佛山市高明区人民医院核心系统信息安全等级保护整改需求说明

我院核心信息系统为 HIS、LIS、PACS，安全等级保护分别拟定三级、二级、二级，本项目需要根据我院现有实际情况对照等级保护标准完成整改，并达到验收测评合格。本次整改，除按完成整改外，还要重点加强网络准入管理、计算机终端桌面管理，对已老化的安全设备：外网防火墙及上网行为管理等进行更新。

整改服务，需要签订合同后，二个月内完成。

## 一、关键性能（不可负偏移）

序号	项目名称	参数	单位	数量
1	网络安全基础服务-1年服务	针对测评的三个系统，包含两次的安全基线检查、安全漏洞扫描、安全加固服务和一次的安全管理制度完善服务。 1、安全基线检查：针对测评的信息系统涉及的主机服务器、网络设备、安全设备进行安全基线检查，查找不安全的配置，并提出优化加固建议，频率：2次。 2、安全漏洞扫描：体内容包括操作系统漏洞、应用软件漏洞、数据库漏洞、网络设备漏洞等，评估后编写评估报告并对漏洞修复提供建议，频率：2次。 3、安全加固服务：针对上诉工作发现的安全漏洞以及等级保护测评发现的安全漏洞、安全隐患，不符合的高风险项目、不安全的基线配置，提供安全加固建议方案，并协助完成安全加固级及等级保护整改工作，频率：2次。 4、安全管理制度完善：根据等级保护三级系统要求，协助用户建立、完善一套符合登记保护三级标准要求的安全管理制度文档，频率：1次。	项	1
2	网络安全应急演练-1年服务	与用户协商确定应急演练预案，组成应急演练小组，组织开展单位内的应急演练工作，并形成记录文件，事后汇总编制应急演练总结报告，频率：1次。	项	1

3	上网行为管理	标准≥1U 机架式设备，吞吐量≥500Mb；并发会话数≥120,000；用户规模≥1400 人；设备接口≥4 个千兆电口，≥2 个千兆光口；硬盘≥1TB；支持 IPSEC VPN 加密性能 50Mb；含系统软件（包含三年的 URL 规则库升级+三年的软硬件质保）	台	1
4	互联网出口防火墙	<p>整机吞吐量≥4 Gbps；配备千兆电口≥6 个，USB 接口数≥2 个，扩展插槽≥1 个，串行管理接口 RJ451≥个，可额外扩展 4 个千兆接口或 8 个千兆接口或 4 个千兆光口或 8 个千兆光口或 4 个千兆接口 4 个千兆光口或者 2 个万兆接口或 4 个万兆接口。标配双电源。；支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及 URL 分类管理、流控和 IPSec VPN 模块；</p> <p>IPS 特征库、防病毒特征库、应用识别及 URL 分类库三年升级服务。</p>	台	1
5	安全运维管理系统	<p>2U 机架式，冗余电源，4 个千兆网口，保修 36 个月；最大支持 2000 台设备的管理；支持基于 NACC、802.1x、E0U、WebAuth、MAB、IAB 等技术的网络准入控制；支持 URL 和 POP3 重定向提醒功能；支持桥接、路由、端口镜像、NAT、FakeDNS 模式；内置 UA-Mgr-1 管理控制中心许可；内置系统所需的操作系统和数据库软件；系统在与互联网隔离的情况下，要实现系统及微软补丁的安全自动更新；支持闲时（鼠标/键盘长时间未操作）终端关机、注销、锁定、重启、睡眠、休眠、关闭显示器等操作；支持对通过数据库工具访问数据库时操作的数据信息的保护。</p> <p>含 1500 个网络准入控制（Windows 客户端、Linux 客户端、安卓、IOS、MacOS 设备、哑终端）许可。</p> <p>含 1500 个桌面管理模块客户端许可。</p> <p>含 200 个终端违规外联控制许可。</p> <p>含 200 个 USB 移动存储介质管理模块客户端许可。</p>	套	1
6	集成实施管理	主要工作包括前期现场调研、制定项目实施方案、制定项目实施计划、划分项目阶段、项目任务分解、项目人员工作安排及与设备第三方人员协调沟通、	项	1

## 二、主要技术参数

### 2.1 上网行为管理

技术指标	技术规格要求
▲通用指标参数	标准≥1U 机架式设备，吞吐量≥500Mb；并发会话数≥120,000；用户规模≥1400 人；设备接口≥4 个千兆电口，≥2 个千兆光口；硬盘≥1TB；电源：单电源；
网关模式	支持网关模式，支持 NAT、路由转发、DHCP、GRE、OSPF 等功能；
所有功能全面支持 IPv6	支持部署在 IPv6 环境中，且其所有功能（上网认证、应用控制、流量控制、内容审计、报表等）都支持 IPv6；（每项功能提供产品界面截图）
管理界面	支持 SSL 加密 WEB 方式、SSH 命令行方式管理设备；
IPsec VPN	必须具有 IPsec VPN 远程加密访问和连接的模块，并能提供 IPsec VPN 客户端授权远程接入访问； IPsec VPN 支持多线路功能，支持配置主备线路组和流量分配模式的多线路选路策略； 支持硬件特征码绑定认证； IPsec VPN 支持与 LDAP 服务器、Radius 服务器结合认证；（提供产品界面截图）
链路负载	支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载；支持使用 VPN 做专线备份；支持链路故障检测；（提供产品界面截图）
▲网络故障检测	实时监控网络异常情况，，支持快速发现内网 DOS 攻击、流量超过设备限制、网口丢包异常、网络不通等影响业务网络的异常情况；（提供产品界面截图）
首页可视化分析展示	支持首页分析显示接入用户人数、终端类型、认证方式；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况；（提供产品界面截图）
Web 访问质量检测	针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持以列表形式展示访问质量差的用户名单；支持对单用户进行定向 web 访问质量检测（提供产品界面截图）
多终端自绑定	同一个账号，支持与指定数量的多个终端进行自动绑定；（提供产品界面截图）
短信认证	支持短信认证方式，用户输入手机号作为用户名，通过短信猫或短信平台发送验证码；短信认证能够根据不同用户推送不同认证页面，该认证页面可自定义，编辑内容包括文字、颜色风格、图片，且图片支持轮询播放；
二维码认证	支持二维码认证，管理员扫描访客的二维码后对其网络访问授权（提供产品界面截图）
自定义用户属性	以针对用户属性配置上网权限策略、流控策略，审计策略等（提供产品界面截图，）

账户有效期及用户密码强度	支持自动删除长期不登录账号信息;可对用户密码强度进行限制,如设置用户密码不能等于用户名;新密码不能与旧密码相同;可设置密码最小长度;可设置密码必须包括数字或字母或特殊字符; (提供产品界面截图)
▲自定义计划任务	支持终端调用管理员指定脚本/程序以满足个性化检查要求,比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等; (提供产品界面截图)
终端准入	支持 win 8 64 位操作系统,支持在旁路模式部署下准入生效;支持禁止不满足终端检查要求的用户访问互联网;支持识别终端操作系统版本、系统补丁安装情况;实现网络流量分析,上网行为管理系统与终端安全防护系统联动,并检测到终端未安装终端安全防护软件后,上网行为管理可以提供重定向到终端安全防护软件下载页面。
补丁检测	支持检测 windows 重要补丁的安装情况,并反馈检测结果; (提供产品界面截图)
应用识别规则库	支持根据标签选择应用,标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖 6 大类;支持给每个应用自定义标签;支持根据标签选择一类应用做控制;支持对每一种应用的定义和解释,帮助客户快速定位应用的分类;支持给每一种应用列上图标,易于客户了解应用的特征。 (提供产品界面截图)
应用控制	设备内置应用识别规则库,支持超过 7500 条应用规则数,支持超过 4000 种以上的应用,1000 种以上移动应用,并保持每两个星期更新一次,保证应用识别的准确率; (提供产品界面截图)
QQ 白名单	支持基于用户组、终端类型、位置的 QQ 白名单功能。 (提供产品界面截图)
共享接入管理 (防共享)	设备能够发现私接路由 (或者共享软件等) 共享网络的行为: 1. 支持自定义配置终端数量和冻结时间,和添加信任列表; 2. 支持显示以 IP 或用户名的维度统计一段时间内的趋势图。 3. 支持例外排除功能: 如指定例外条件 1 台 PC, 2 个终端。当 PC 或终端数超过例外条件才会被判定为共享。 (提供产品界面截图)
加密 SMTP 邮件过滤	支持对加密 HTTPS、SMTP-SSL、SMTP 的邮件进行关键字过滤; (提供产品界面截图)
加密 SMTP、POP3 邮件审计	支持对加密 HTTPS、POP3-SSL、POP3、IMAP、IMAP-SSL、SMTP-SSL、SMTP 邮件内容的审计。 (提供产品界面截图)
上网流速提醒	用户指定应用上网流速超过预设阈值后,网关自动提醒该用户; (提供产品配置界面)
带宽管理	必须支持在不同线路上,根据不同的应用、用户/用户组、位置、终端类型来保证或者限制流量;支持根据百分比或数值设置通道带宽,并支持设置各通道的优先级;

▲流控通道实时可视化	能够实时看到各级流控通道的状态:包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽、优先级,启用状态等。(提供产品界面截图)
P2P 智能流控	支持通过抑制 P2P 的上行流量,来减缓 P2P 的下行流量,从而解决网络出口在做流控后仍然压力较大的问题;(提供产品界面截图)
流控黑名单	基于“流量”、“流速”、“时长”设置配额,当配额耗尽后,将用户加入到指定的流控黑名单惩罚通道中(提供产品界面截图)
移动终端管理(非法 Wi-Fi 热点管控)	设备必须支持能自动发现网络中通过无线上网的热点和移动终端的 IP 和终端类型;支持管理员配置热点信任列表;支持发现信任列表外非法接入的热点和终端,并阻止该热点/终端上网;支持将非法热点接入网络的行为通过邮件告警通知管理员,并在数据中心支持行为记录和查询;支持以图表方式显示移动终端接入趋势;(提供产品界面截图)
防火墙	必须能防范三层网络环境中的 ARP 欺骗问题;必须具有防火墙功能模块;
加密证书自动分发	审计 SSL 网页时,支持加密证书自动分发功能,用户点击网页上的工具即可一次性安装完成。解决管理员给每台 PC 单独安装证书的问题(要求提供产品界面截图)
数据中心	设备必须支持内置数据中心和独立数据中心(提供产品界面截图);
高性能日志模式	支持日志高性能模式处理,精简冗余日志(提供产品界面截图);
单用户行为分析	针对单用户的行为分析(包括:应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等)(提供产品界面截图)
关键字订阅	支持预置几组关键字,当审计日志中出现这些关键字时,将定期以邮件的方式发送报告给指定邮箱(提供产品界面截图)
网络整体状况报表	从带宽健康分析、工作效率分析、离职风险分析、合规性分析四个大块对网络整体状况进行说明
离职风险报表	从用户上网行为的多个维度(如访问网站、搜索关键字等)分析员工的离职风险
支持与多种网安日志平台对接	内置多套日志模板与各省市网安日志平台对接,至少支持以下平台:派博、任子行、网博、云辰、烽火、中新软件、兆物、新网程、美亚柏科、爱思等。
应用商店展示	可以支持以应用商店的形式发布各种数据分析应用;支持直接展示已安装和未安装的应用,支持选择安装或卸载应用;支持直接展示应用更新列表,可选择是否更新当前已安装应用;(提供每个功能点提供截图证明)
全网上网态势分析	在地图上显示所有各分支地理位置,点击图标能够单独显示当前分支网络现状(用户情况、带宽情况、应用情况等);支持图形形式,动态显示整体上网态势,包括:总体应用流速趋势、应用流量分布、用户流量分析;(提供功能截图证明)

办公网上网态势分析	支持图形形式，动态显示整体上网态势，包括：总体应用流速趋势、单位流量分布、应用流量分布、热门应用排行等；提供自定义配置显示模块，对需要显示的模块内容勾选即可；（提供功能截图证明）
泄密追溯分析	支持分析整体外发风险概括，包括外发敏感文件的总次数、文件类型、外发通路等状况；支持泄密行为追溯，可以上传文件和关键词，查询有过相关外发记录的人员，通过相似度匹配给出风险人员排行；
工作效率分析	支持整体工作效率分析，展示整体的日均工作无关时长和总工总人数，以及工作无关应用时长趋势；支持部门分析，包含影响因素分析、影响时段分析、工作效率趋势分析、总工人员分析；（提供功能截图证明）
离职倾向分析	可查看具有离职倾向人员的判定依据，判定依据从简历投递、访问求职网站等多个维度综合判定；支持按离职风险等级划分，分为高风险人员和疑似人员；支持指定具体用户进行搜索，判定具体的人员是否存在离职倾向；（提供功能截图证明）
产品相关认证	▲公安部颁发的《网络通讯安全审计产品 销售许可证》
	公安部颁发的《互联网公共上网场所 信息安全管理系统（无线接入前端）销售许可证》
	国家网络与信息系统安全产品质量监督检测中心《信息技术产品安全分级评估证书-评估保证级 3（EAL3 级）》
	中国信息安全认证中心 ISCCC《IT 产品信息安全产品认证证书》
	具有工信部颁发的《电信设备进网许可证》
	IPv6 Ready Phase-2 认证

## 2.2 互联网出口防火墙

系统架构	采用专用多核硬件平台
▲硬件规格	必须配备千兆电口 $\geq 6$ 个，USB 接口数 $\geq 2$ 个，扩展插槽 $\geq 1$ 个，串行管理接口 RJ451 $\geq$ 个，可额外扩展 4 个千兆接口或 8 个千兆接口或 4 个千兆光口或 8 个千兆光口或 4 个千兆接口 4 个千兆光口或者 2 个万兆接口或 4 个万兆接口。标配双电源。
▲性能	防火墙整机吞吐量 $\geq 4$ Gbps。
	每秒新建 HTTP 连接数 $\geq 10$ 万/秒
	最大并发连接数 $\geq 220$ 万
访问控制	▲支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略，提供相关界面截图
	▲支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。提供相关界面截图
	▲支持基于基于 IP、用户、应用参数及应用内容的应用行为许可控制。提供相关界面截图

	支持路由、透明及混合部署模式
	支持常见 DOS 攻击防护及 ARP 攻击防护
	支持基于协议的长连接管理
行为管理及流量控制	支持基于 DPI 和 DFI 技术的应用特征识别及行为控制，应用识别的种类不少于 1000 种
	支持基于线路和多层通道嵌套的带宽管理
	支持基于接口的上下行带宽管理
	支持高、中、低优先级通道设置
	支持基于应用、用户、源地址、目标地址、服务、时间的通道匹配
	支持带宽限制、带宽保障和弹性带宽
网络特性	支持静态路由、动态路由（RIP、OSPF、BGP4），提供相关界面截图。
	▲支持基于入接口、源地址、目标地址、服务端口、应用类型的策略路由。提供相关界面截图。
	支持链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法，提供相关界面截图。
	▲支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性的多重健康检查，提供相关界面截图。
	支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT
	支持各种应用协议的 NAT 穿越：FTP、TFTP、H. 323、SQL * NET
	支持标准 DHCP 服务功能，支持 DHCP 条件下的 IP/MAC 绑定及 IP 地址排除等功能。
	支持标准 DNS 服务器功能，支持多种 DNS 记录，包括 A，NS，CNMAE，TXT，MX，PTR 记录。
高可用性	支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。
	支持基于心跳信号丢失、链路断开等多种方式的 HA 切换条件及逻辑
	支持 HA 设备之间的会话自动同步，确保 HA 切换时业务不发生任何中断
	支持 HA 设备之间的配置自动同步，确保用户只需在一台设备进行业务配置
防病毒	支持应用协议自识别，可以实现 HTTP，FTP，POP3，IMAP，SMTP 多种应用协议下的病毒防护，可自定义文件类型。
	支持路由、透明、混合等各种工作模式下的网络病毒检测
	支持基于病毒防护规则，可以实现放行、阻断。
	病毒库不少于 1200 万种病毒特征
产品资质	▲产品具备计算机信息系统安全专用产品销售许可证-增强级；提供有效的资质证明复印件。
	产品具备国家信息安全测评自主原创产品测评证书；提供有效的资质证明复印件。

	产品具备商用密码产品型号证书，提供有效的资质证明复印件。
	▲产品具备国家信息安全测评信息技术产品安全测评证书 EAL4+；提供有效的资质证明复印件。
	产品具备中国国家信息安全产品认证证书，提供有效的资质证明复印件。
	产品具备 IPv6 Readylogo Phrase 2 认证；提供有效的资质证明复印件。
服务能力	▲产品厂商具备国家级网络安全应急服务支撑单位资质证书。需提供有效资质证明复印件。
	为确保项目安全性、机密性，产品厂商必须具备涉密信息系统集成资质证书（甲级系统集成及软件开发）。需提供有效资质证明复印件。
	▲产品厂商为微软 MAPP 计划成员单位，第一时间获取漏洞信息，实现安全防御。需提供有效证明文件。
	▲所投产品厂商具备信息安全漏洞发掘能力，实现对产品的检测防御，提供自主挖掘的 CVE 漏洞发现数不低于 400 个。提供自主挖掘 CVE 列表。
	所投产品厂商具备信息安全相关专利技术，提供自主专利数不低于 100 个。提供列表证明。

## 2.3 安全运维管理系统

技术指标	技术规格要求
硬件参数	支持 1500 台设备的管理
	设备需要自带操作系统；
	设备需要自带数据库；
	设备需要自带双机热备软件；
	设备需要有自主知识产权，须为标准机架式硬件产品；
	设备至少需要配置 4 个 1000M 网口，配置独立的 1 个 Console 接口；
基本参数	管理后台要求支持中文界面及联机中文帮助，客户端要求支持中文（包括简体和繁体）、英文；
	以下功能一个厂商的一个产品即可支持，不需要通过多个产品集成实现；
	要求客户端进程数不超过 2 个，所有进程所占用内存不得超过 30M，CPU 正常情况下占用不得超过 3%；
	▲系统在与互联网隔离的情况下，要实现系统及微软补丁的安全自动更新；
网络环境支持	支持混合厂商大规模网络环境，例如 Cisco、H3C、华为、锐捷、迈普、Nortel 等厂商的网络设备环境；
	支持跨越路由器、VPN、防火墙等复杂环境；



	支持自动发现接入网络的所有网络设备、主机、桌面 PC、其他 IP 设备之间的二层连接关系，如：发现交换机之间通过什么端口相互连接，发现每台桌面 PC 是连接到哪台交换机的哪个接口上；
	支持自动发现接入无线网络的终端，可以发现设终端所连接的 SSID 信息；
拓扑性能要求	即使终端开启个人防火墙或安装其他防火墙软件，也可以进行自动发现；
	提供拓扑连接图，并支持图形编辑和自动排列功能；
	提供拓扑关系的表格展示，方便查询定位设备连接到哪台交换机的哪个端口上；
	保证外来 PC、笔记本（没有 Agent）接入网络时能被及时发现，并通知系统管理员；
网段信息统计	支持对发现过的网络信息，根据子网掩码进行网段自动汇总，并对网段中 IP 占用情况进行图形化展示；
设备快速定位	要求可以依据如下信息对接入网络的设备进行快速定位，包括但不限于设备的 IP 地址、MAC 地址、主机名、用户名；
	快速定位设备时，必须找到设备所直接连接的网络交换机端口及对应的信息点编号；
	可以依据某台设备或终端的历史上曾经使用过的 IP，对该设备进行定位；
	自动发现、定位网络中非法接入的 HUB、无线 AP 等设备，找到这些非法设备通过哪台网络设备的哪个接口接入；
	当设备从一个网络接口移动到另外一个网络接口，系统可以在 1 分钟内被发现；
	可以发现内部网络是否与其它网络非法连通，并对其进行定位；
	设备快速定位不依赖安装客户端，要求未安装客户端的设备也能够进行定位；
组织架构管理	可以根据终端的 IP 使用情况，快速判断并定位到使用 NAT 网络接入内网的设备；
	支持自动同步企业 AD/LDAP 上的组织架构部门信息、用户账号信息、设备信息；
	支持手工维护组织架构部门和成员信息，允许通过导入导出操作进行批量维护；
	支持设置多级部门，子部门关系级数无限制；
	部门用户信息应包含但不限于工号、全名、备注、所属部门、联系方式（电话、手机号、邮件地址、Windows Message）；
	部门设备信息应包含但不限于设备名、IP、MAC、网络设备，端口；
	允许将组织架构中任意成员指定为系统管理员；
系统自监控	允许分配 IP、网段和设备给指定部门；
	支持在控制台对后台服务器的注册、编辑、查询等管理动作；

	支持对已注册设备进行监控维护，可维护信息包括服务器名称、IP 地址、当前版本、运行状态、磁盘空间、CPU 负载、内存使用率；
	支持系统自检，自动检查系统的运行状态，发现问题并以低、中、高三个级别通知管理员，保证系统的高可用性；
	支持在控制台查看后台服务、进程运行状态，并可手工进行启动/停止等维护操作；
	支持在控制台查看后台服务器的版本信息及注意事项；
	支持对后台服务器的时间进行同步设置；
	支持对多套系统进行集中管理、软件包集中升级；
网络接入场景	一套准入控制系统同时支持有线、无线、VPN、HUB、NAT、漫游、远程分支机构接入等多种方式进行管控；
	支持对 PC、瘦终端、哑终端等设备通过网线连接交换机接入企业内部网络时进行准入控制；
	支持对手机、PAD、笔记本等移动设备通过无线以太网卡连接 WLAN 接入企业内部网络时进行准入控制；
	支持终端设备在外部互联网环境通过 VPN 手段接入企业内部网络时进行准入控制；
	支持多个终端设备通过同一个 HUB 接入企业内部网络时进行准入控制；
	支持设备通过路由器等设备进行 NAT 转换 IP 后接入企业内部网络时进行准入控制；
	支持设备通过远程分支机构接入企业内部网络时进行准入控制；
	支持设备在无需重新安装客户端的情况下，漫游至其他分支机构接入企业内部网络时进行准入控制；
	一套系统、一个客户端支持所有接入方式，终端在不同的场景间无缝切换；
	支持根据网络设备、用户、部门、网段、IP 地址灵活配置接入管控策略；
未装客户端	支持有客户端、无客户端、Portal 等方式接入；
	支持对未安装客户端的电脑进行自动重定向式引导，提醒并帮助用户自助安装（需要提供系统截图）；
	支持 HTTP 协议、HTTPS 协议的页面重定向、发送 Email 邮件等形式进行引导；
	支持对企业内部指定的免检设备通过 IP 或 MAC 地址进行准入放行操作；
	支持通过 OS 内置客户端的设备进行准入认证；
已安装客户端	支持通过浏览器访问页面进行准入认证；
	支持对已安装客户端的设备进行身份认证，允许合规用户接入网络；
	支持 LDAP、AD、内置账号、Mail、数据库等不同的身份认证源；

	支持客户端与企业 AD 域联动，自动获取终端账号并接入网络，该过程终端用户没有感知；
	支持对检查过程中存在安全漏洞的计算机，隔离出工作网络，并提供修复区，引导用户自助修复；
准入身份认证源	能自动同步 AD/LDAP 上的组织架构信息和用户帐号信息，组织架构信息用于设置用户的资源访问权限；
	准入身份验证必须支持微软 AD 域帐号、LDAP 帐号、X.509 证书、内置账号和外部第三方 Radius 等；
	要求 CA 认证源可以同步 AD 域等第三方认证源；
	需要支持身份验证凭据（USB-KEY 或 AD 账号）与计算机 MAC 地址、接入交换机端口号、客户端软件随机认证码、终端硬件唯一 ID、认证用户等进行灵活绑定，并可以满足一对多、一对一、多对一、多对多绑定；
	需要针对外来用户、不同单位用户的临时接入进行管理，当外来用户或不同单位用户需要临时接入网络时，可以授权管理员或合法用户进行登记、授权、放行，放行可针对 MAC、IP、时长等进行控制。
	支持通过手机号获取动态码认证
	需要支持微信准入，即访客或内部员工通过微信验证接入网络
	支持二次开发与企业短信平台进行联动
准入安全检查	支持二次开发与企业 OA 等系统实现统一验证
	接入帐号的合法性，接入的硬件信息，包括 MAC 地址、主机硬件标识等；
	接入设备的安全设置，防病毒软件的安装与更新信息，必须要支持现有防病毒客户端的准入检查；
	Guest 来宾账户检查、弱口令账户检查、AD 域用户检查、共享目录检查；
准入控制绑定	系统补丁检查、注册表项检查、文件要求检查、软件配置检查、软件组配置检查、准入客户端的企业标签
	支持终端信息与用户信息、网络设备信息一对一绑定，校验绑定认证；
	支持用户和 MAC 地址绑定；
	支持用户和交换机端口绑定；
	支持用户和接入控制点绑定；
	支持在无线 802.1x 准入环境下用户和 ssid 绑定；
	支持在无线 802.1x 准入环境下 MAC 和 ssid 绑定；
	支持通过 excel 导入导出方式维护绑定对应关系；
入网权限控制	能够根据管理员设置的条件进行自动绑定放行，并可以指定自动绑定数量
	准入系统能够根据用户、部门和设备设置接入网络访问权限（ACL）；
	权限控制需要支持交换机、无线 AC、自主的硬件网关；

	<p>准入系统能够自动判断打印机、网络摄像头、IP 电话，并对这些设备进行自动入网授权，网络访问权限按照设备类型分配，实现最小化（仅访问实际需要访问的资源）。</p> <p>▲能够区分同一用户使用客户端和使用 Web 认证的网络访问权限。以免权限释放过大（提供系统配置截图）；</p>
终端发现和识别	<p>系统能够即时发现接入网络的终端，信息包含：接入设备 IP、接入设备 MAC、接入的交换机端口、使用设备的用户。</p> <p>系统能够准确的自动识别常见的 Windows、Linux、MAC OSX、IOS 和 Android 系统，并可以生成易于管理的树形结构设备列表。（提供系统截图）</p> <p>系统能发现网络中常见的 IOT 设备，需要至少支持：打印机、网络摄像头、IP 电话。同时能够根据终端行为进行设备自动分组。</p>
行业标准技术 IEEE 802.1x	<p>支持基于有线（与接入层交换机联动）802.1x 的网络准入方式</p> <p>支持基于无线（与无线控制器联动）802.1x 的网络准入方式，无需第三方 RADIUS 服务器支持</p> <p>支持 802.1x 技术下 IP 电话 Voice VLAN 授权技术</p> <p>支持 802.1x 动态 VLAN 授权技术（Guest VLAN、修复 VLAN、工作 VLAN）</p> <p>支持 802.1x 动态 ACL 授权技术</p> <p>支持 802.1x 技术下 IP 电话串接电脑场景</p> <p>支持 802.1x 技术下终端通过 HUB 接入场景</p> <p>支持 802.1x 技术下通过 MAC 地址旁路接入场景</p>
企业标准技术	<p>支持策略路由方式准入</p> <p>支持端口镜像方式准入</p> <p>支持 Cisco EoU 方式准入</p> <p>支持 DHCP 方式准入</p> <p>支持 Fake DNS 方式准入</p> <p>支持 Portal/Portal+（与网络设备和 AC 联动）方式准入</p> <p>关闭 Portal 认证页面后能够自动下线</p>
准入重定向引导	<p>支持终端入网浏览器重定向引导，当用户访问网页时能够自动转向到指定的页面或地址</p> <p>支持 HTTPS 重定向引导，当用户访问 https 网站支持支持自动跳转到指定的页面或者地址</p> <p>支持根据用户的实际环境自定义非 80 端口的 Web 服务端口号及用户重定向引导</p>
终端在网安全检查	<p>支持对在线终端的网络流量、上网特征实施检查，一旦行为发生异常，需要立即隔离出网络；</p> <p>支持对指定终端的心跳进行检测，一旦发现心跳中断，需要立即隔离出网络；</p> <p>准入系统能够检测出通过 IP / MAC 伪装方式接入网络的行为，并将伪装终端隔离出企业网络。</p>
智能准入	<p>能够识别出指定类型的终端，并要求对指定类型的终端进行准</p>

	入控制。
NAT 设备发现	支持 NAT 识别和检测机制能够及时发现网内私接的小路由器、无线 AP、随身 WIFI 等 NAT 设备，帮助清查通过网中网隐藏的真实网络终端
	支持根据 NAT 设备查找到 NAT 使用的外部地址，连接的交换机和交换机端口
NAT 认证	支持对 NAT 入网的计算机实现准入控制、安全评估和修复检查
▲访客接入管理	准入系统支持访客接入，提供页面填写申请单方式（申请单内容可以自定义）。 访客系统支持：系统匹配受访人信息自助接入、受访人审核和系统管理员审核接入模式，以满足不同的管理需要。（需要提供系统配置截图）
	准入系统能够根据访客类型进行网络动态授权。确保访客网络访问权限最小化。（需要提供系统配置截图）
外协接入管理	准入系统能够提供驻场外协用户接入，并可以根据外协公司设置网络访问权限。（需要提供系统配置截图）
集中管理	系统支持数据集中展示，支持将下级信息上报到上级进行统一展示
	系统支持数据集中管理，支持通过上级直接管理下级系统
	系统升级管理，支持从上级发布升级包到下级系统
系统监控	系统拥有自监控模块，能够检测系统硬件资源使用情况，系统模块可用性检测
	系统支持第三方监控平台，支持通过 SNMP 监控、支持 Zabbix 监控
系统工具	支持通过 Web 管理界面提供 ping、抓包、traceroute 等功能，并可以设置命令参数进行相关调试。
智能终端接入	准入系统支持 PAD、iPhone、Android 常见移动智能终端接入。
	准入系统需要兼容主流网络设备，802.1x 和 Portal 技术至少需要支持：思科、华为、华三、锐捷、迈普五个常用品牌的网络交换机和无线 AC、AP 设备。（需要提供使用客户案例）；
	▲准入客户端需要兼容企业常用的操作系统，WindowsXP / 7 / 8 / 10，MacOSX、Ubuntu 桌面系统、IOS、Android（需要提供客户端运行截图）；
	使用 Web 认证方式，需要具备一次认证多次有效，要避免用户频繁的输入账号密码方式，在保证体验的前提下，同样需要保证接入安全
单点登陆（SSO）	▲支持与深信服上网行为系统单点登陆，准入认证通过后，无需再进行上网行为系统认证
性能	准入系统处理认证请求速度应大于 1000 个 / 秒，以满足高并发需要（需要提供测试报告和测试方法）。
	网关式准入控制器，数据包转发速度应该小于 50us，网络吞吐量不小 1GB，认证处理速度应大于 1000 个 / 秒（需要提供测试报告和测试方法）

易用性	系统应自带帮助功能，以帮助管理员对系统的理解和操作；
	系统应该提供的接入记录应该清晰显示：接入状态、接入时间、接入用户、接入设备。接入失败的记录需要提供详细的失败原因，管理员可以快速判断失败原因；
可靠性	系统需要支持双机部署方式（HA），确保高可用性；
	主备服务器的数据需要时刻保持一致，数据同步时间应低于 30 秒，以确保备机能够及时代替主机运行；
	系统需要支持自动 / 手动的应急方式，系统检测到运行中出现的异常和故障需要能够自动应急，确保企业网络的可用性；（需要提供简要说明）
	系统需要提供本地备份、网络备份和异地备份方式，在系统出现故障后，能够快速恢复到最近的备份状态；
	系统能够对自身的运行状态进行健康检查，并定期提供检查报告，可以用于系统巡检；
补丁下载	支持微软 WSUS 补丁服务器，同时也支持独立的补丁服务器，能够自动从微软网站下载补丁，或者通过拷贝方式将补丁导入到补丁服务器；
	补丁可以支持推、拉的安装方式，能够按照 OS 版本、补丁级别、补丁是否经过审批、终端设备所在部门或其他分组条件决定补丁是否要在某台设备上安装。支持补丁的卸载和回退；
	支持云补丁部署，快速检查终端补丁安装情况，不依赖于 Windows update；
补丁分发	支持分级分发，即一级服务器将补丁下发给各二级服务器，二级服务器下发给所管理的终端；
	支持补丁分发对带宽、对业务终端性能的影响；要求补丁分发时，可以指定分发的开始时间、结束时间；
	对补丁分发带宽占用进行优化：对于分支当地没有服务器的情况；
	支持补丁分发时意外中断后的断点续传；
补丁安装	支持客户端自动检测并自动从服务器下载补丁安装；
	支持客户端手工选择需要安装的补丁，然后安装；
	在整个打补丁的过程中终端用户不受打扰，不需要做任何设置和操作；
	管理后台操作需要简单，一次点击，就需要确保所有终端全部自动打上最新补丁；需要从多个角度、纬度展现补丁的安装情况。
	快速及时的检查出所有需要安装的补丁。3 秒内检查出系统所需要安装的所有补丁。1 小时内自动给 1500 个终端打上补丁；
	支持补丁分发时意外中断后的断点续传；
	支持蓝屏修复；
	能自动统计终端补丁程序安装率，并提供补丁分发报表；
	分别从补丁，或终端角度查看、统计补丁安装情况；
资产采集	支持终端软/硬件信息、服务信息、进程信息采集；支持终端

	计算力评估;
	支持采集主板、BIOS 信息、CPU 信息、光驱、硬盘信息、显卡信息、声卡信息、网卡信息、显示器信息、内存信息;
远程协助	远程协助, 必须经过终端用户同意后, 管理员才可以上到终端用户系统界面
	远程监控, 管理员直接上到终端用户系统界面, 不需要终端用户同意
	请求协助, 终端用户可主动请求管理员远程协助
	多对一协助, 多个管理员可同时对一个终端用户进行协助
	协助消息, 在远程监控与协助过程中, 管理员可与用户进行消息对话;
	远程截屏, 在远程监控与协助过程中, 管理员可对终端桌面进行截屏操作
	待处理请求: 此处可以查看申请远程协助请求的请求人详细信息, 以及管理员可以对此次请求做出“协助”、“拒绝”、“导出”的动作
	远程协助历史: 可查看远程协助的历史详细信息 (包括由管理员发起的、客户端发起的)
	远程协助: 支持带宽自动优化功能; 支持远程传送文件功能; 服务端和客户端都能主动发起呼叫;
	支持对管理员的远程会话审计/录像审计功能;
	支持 NAT 环境下远程协助, 即被协助终端位于防火墙后面也必须可以远程协助;
	支持 MAC 终端远程协助
节能管理	节能管理: 支持终端闲时节能措施;
	▲支持闲时 (鼠标/键盘长时间未操作) 终端关机、注销、锁定、重启、睡眠、休眠、关闭显示器等操作;
	支持终端解除节能申请;
	支持能耗报表统计;
U 盘管控	可对普通移动存储介质的使用进行管控, 包括禁用、使用审计等管理;
注册 U 盘	提供终端自主注册流程, 提供按设备、部门、用户等多组合使用范围控制;
非法外联控制	提供终端设备的外联接口进行安全管控, 包括但不限于红外、蓝牙、软盘、光盘、串口、并口、网络接口、USB 接口以及其他外联设备;
	提供智能设备连接控制, 禁用时可提供充电服务;
	支持终端连接互联网的审计和控制;
	支持禁用终端电脑共享 WiFi 热点;
	提供 U 盘内可执行文件控制, 避免 U 盘自运行程序;
保护对象	支持对基于 IP、端口访问 B / S 或 C / S 架构的业务系统时操作的数据信息的保护;
	▲支持对通过数据库工具访问数据库时操作的数据信息的保

	护;
	支持对通过 Telnet/SSH 服务访问网络设备时的数据信息的保护;
	支持对局域网内终端共享流转文件的数据信息的保护;
	支持对以文件形式存储在终端的数据信息的保护;

#### 四、付款方式要求

- 1.货物到位后 30 天内，支付 30%。
- 2.项目验收（所有项目实施完成，且收到评测服务机构出具合规的验收测评报告）后 30 天内，支付 60%。
- 3.验收 1 年后 30 天内，支付 10%。

#### 五、售后服务要求

- 1.提供 3 年质量保证期，质量保证期内所有硬件设备的故障维修均为免费。
- 2.提供 5×8 免费硬件维修服务，同代软件版本升级服务（包含三年的 URL 规则库升级），5×8 热线技术支持服务。
- 3.提供每天 5×8 小时的备件更换服务，在报障的次日更换备件。
- 4.提供每天 5×8 小时的现场支持服务，硬件更换、现场问题处理服务，在报障次日到达现场。
- 5.在备件停止生产的情况下，需事先将要停止生产的计划通知用户，使用户有足够的时间采购所需备件。
- 6.注明其它质保期满后，具体需收费情况及服务标准。