**零信任安全网关技术参数**

1、支持软件模式部署交付；零信任接入授权≥600套，客户端沙箱授权≥200套。

2、通过隧道模式，可以支持基于TCP、UDP、ICMP等协议代理访问业务资源，支持发布IP、IP范围、IP段、具体域名及通配符域名等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面。为简化资源发布配置，隧道模式应支持同一个资源发布多个服务器地址；管理员还可基于业务的特殊性，自主选择优先使用长连接或短连接进行业务代理；

3、在业务应用兼容性良好的情况下，支持以隧道模式发布http/https协议的资源，以增加在隧道模式下发布的资源的URL级别审计能力，同时支持为隧道资源添加WEB水印以及单点登录功能。

4、应支持配置应用资源指定的打开方式，如浏览器等；为了适应某些业务系统对浏览器的兼容性，还应支持配置应用打开的指定浏览器类型；

5、为了最大程度缩小网络、业务暴露面，零信任平台需提供单包授权能力（SPA），支持UDP+TCP组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口，不会出现敲门放大漏洞。安全码支持一人一码模式，支持短信分发安全码，保障业务的安全性。

6、为了保障员工顺利访问经零信任隧道模式代理的业务，零信任客户端应兼容主流非国产终端，包括但不限于：Windows7（32位、64位）、Windows10（32位、64位）、Windows11（32位、64位）、MacOS10、MacOS11、MacOS12、Android、iOS等非国产操作系统的终端；

★7、为了保障用户在国产化终端上的正常业务访问，零信任客户端应兼容主流国产硬件CPU的国产操作系统终端，需提供国产操作系统与零信任厂商的兼容性证明，包括但不限于麒麟V10×龙芯、麒麟V10×龙芯LoongArch、麒麟V10×飞腾、麒麟V10×鲲鹏、麒麟V10×兆芯、麒麟V10×海光、麒麟V10×海思麒麟；统信V20×龙芯（3A3000、3A4000）、统信V20×龙芯（3A5000）、统信V20×飞腾、统信V20×鲲鹏、统信V20×海光、统信V20×兆芯等；（提供兼容性证明证书并加盖厂家公章）

★8、为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：帐号首次登录、帐号在该终端首次登录、闲置帐号登录、弱密码登录、异常时间登录、非常用地点登录等；（提供产品功能截图并加盖厂家公章）

★9、支持以文件为单位，对工作应用产生的数据进行加密保存；文件加密支持“一文一密”即每个文件独立密钥，以确保沙箱组件被卸载、模块驱动被摘除的情况下，终端用户仍无法明文取出文件；（需提供产品功能截图及公安部计算机信息系统安全产品质量监督检验中心出具的检测报告证明并加盖公章）

★10、支持以列表形式，查看用户在指定时间段内的用户行为数据。显示内容有：时间、用户名、操作对象、本机IP、IP地址归属地、事件类型、命中策略、命中规则名、终端名称、日志上报来源等信息；（要求提供配置截图证明）

★11、支持按用户关键字进行全局搜索、按关键条件组合过滤和日志类型过滤。（要求提供配置截图证明）

★12、为满足医院后续平滑扩容要求和不受硬件性能瓶颈限制，需支持部署在医院当前虚拟化平台，同时为保障系统稳定性，需提供虚拟化厂商兼容性承诺函并加盖公章**。**

13、其他要求：

(1)、含500套零信任接入授权，200套客户端沙箱授权；

(2)、含三年软件升级维保服务。

**多维终端安全管理系统技术参数**

1、基于linux开发的嵌入式专用系统，支持软硬件一体或虚拟化部署；含500个终端管理授权。

★2、客户端支持自定义，包括但不限于是否显示客户端图标、自定义客户端名称、客户端安装包名称是否加密、是否启用万能卸载码等；

★3、客户端版本支持逐步升级，管理员可自定义全部、部分网段更新或禁止指定网段更新的策略；

4、支持针对违规外联、修改系统时间、PC资源使用异常等异常行为进行预警；管理员可自定义违规策略处置策略，包括但不限于报警、断网、锁屏、关机、消息提示、截屏 、代理修复等，并支持自定义策略等延后时间；

5、支持包括但不限于流量、进程、截屏、文件、协议、账户、邮件、打印、服务、共享、注册表、刻录等行为的审计；

6、支持终端安全基线检查，包括但不限于计算机名称、是否加入域、密码策略、弱口令、软件黑白名单、进程黑白名单、系统服务、系统共享等基线检查。提供自动修复功能；

★7、支持主流的杀毒软件版本、病毒库和运行情况的检查，包括但不限于微软MSE、火绒、安天、天融信、赛门铁克、瑞星、卡巴斯基、金山毒霸、江民、NOD32、360、天擎、趋势、小红伞、可牛、windows defender等，支持自动修复功能；

8、支持usb口禁止接入、仅准许接入非存储介质策略；

★9、支持存储介质使用在线审批，终端用户在线发起申请，管理员在线审批、下发策略。策略包括但不限于强制分区、加密、读写权限限制、禁止可执行文件自运行；

10、能够实时监测终端IP地址、MAC地址、DNS配置等相关网络信息，支持对应信息的实时绑定，当IP或MAC发生改变时能够强制恢复至修改前；

★11、管理员计算机与被管理计算机采用专用tcp端口进行直接连接，远程协助时不占用服务器端口资源。远程协助支持双向穿透NAT或VPN的远程屏幕控制；

★12、支持以截图的形式录制计算机的操作录像，支持以视频的形式播放，支持快进、快退、暂停、播放速度调节；

13、能够支持可执行程序、MSI安装包或者文档数据文件自动下发与安装；

14、支持根据操作系统不同分发不同升级包，提高软件分发功能对操作系统系统的适应性；

15、支持远程开启计算机，支持定时、批量开启计算机。

16、其他要求：

(1)、含500个终端管理授权。

(2)、含三年软件升级维保服务。