**中国医学科学院肿瘤医院**

**移动应用安全加固**

**技术需求**

**信息中心/计算机室**

**2019年4月**

目录

[第一部分：项目需求 3](#_Toc5870804)

[1.1. 项目背景 3](#_Toc5870805)

[1.2. 项目描述 3](#_Toc5870806)

[第二部分：技术需求 4](#_Toc5870807)

[2.1. 配置清单 4](#_Toc5870808)

[2.2. 产品技术要求 5](#_Toc5870809)

[第三部分：资质与服务要求 7](#_Toc5870810)

[3.1. 必要资质要求 7](#_Toc5870811)

[3.2. 非必要资质要求 7](#_Toc5870812)

[3.3. 服务要求 7](#_Toc5870813)

第一部分：项目需求

1. 项目背景

近些年来，随着智能手机的普遍应用和移动互联网的飞速发展，用户已逐渐形成了移动互联网思维，习惯了使用智能手机，习惯了使用移动App。移动互联网思维催生了用户对办公移动化的诉求。

为了提升了医院办公效率，我院已经部署了OA办公系统，后续仍会有相关系统需要移动化办公。通过对移动应用的安全加固，打造一套满足使用需求的、安全的、高体验的移动办公环境。

1. 项目描述

要满足移动APP使用的需求，面临着需要将应用服务器发布在互联网上，这就意味着服务器将会承担着互联网的巨大威胁。服务器的 IP 信息暴露，将使得黑客可以通过扫描手段探测服务器， 发现可用的操作系统、中间件、数据库、应用服务的脆弱点，进而采用攻击和入侵手段，窃取敏感数据。因此必须采取一定的安全措施，既满足移动APP访问的需求，又能避免将服务器直接发布到互联网上。

用户使用智能手机通过移动APP访问院内系统，智能手机首先必定是需要通过4G或无线接入互联网，然后使用移动APP与服务器进行数据交互，互联网环境极其复杂，明文方式的数据传输过程也极有可能受到中间人攻击，面临数据泄密、篡改、破坏的风险，因此必须保障用户的远程接入安全，满足数据传输加密、防中间人攻击等安全传输要求。

办公移动化之后，一部分医院数据将通过APP存储在用户手机上，如不进行有效的管控，将会使医院敏感数据面临极大的泄密风险，因此应采取有效的手段保障业务数据与个人应用数据隔离，采用存储加密的方式，防止数据被恶意破解，并且限制用户通过复制粘贴、分享等手段，将敏感信息外发泄密。

第二部分：技术需求

1. 配置清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **配置描述** | **数量** |
| 1 | 主设备 | 配置描述：标准2U尺寸设备，标配千兆电口≥6个，千兆光口≥2个，吞吐量≥2Gbps，理论并发会话数≥160万，SSL VPN最大加密流量≥400Mbps，移动安全接入性能≥450Mbps移动终端安全接入数≥2800个，每秒新建用户数≥300个/秒，标配单电源。支持集群部署，开启企业移动管理模块。产品必须支持经过集成的，基于Android IOS平台的第三方软件开发包（SDK），支持针对移动APP的VPN安全代码的自动封装，实现App应用的安全加固。 | 2台 |
| 2 | 软件授权 | 移动终端接入授权 | 3000个 |

注：所有实现项目功能需求所涉及的证书、配件等，质保期内院方不再增加资金投入，均由投标方提供。

1. 产品技术要求

|  |  |
| --- | --- |
| 指标项目 | 指标要求 |
| 性能要求 | 标准2U尺寸设备，标配千兆电口≥6个，千兆光口≥2个，吞吐量≥2Gbps，理论并发会话数≥160万，SSL VPN最大加密流量≥400Mbps，移动安全接入性能≥450Mbps移动终端安全接入数≥2800个，每秒新建用户数≥300个/秒，标配单电源。支持集群部署，开启企业移动管理模块，两台总计实配3000个移动接入授权。 |
| 部署方式 | 支持网关模式、单臂模式部署两种方式； |
| 基本特性 | 采用标准SSL、TLS 协议，同时支持IPSec VPN、SSLVPN两种VPN，非插卡或防火墙带VPN模块设备；支持对基于HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH等的所有B/S、C/S应用系统，支持基于TCP、UDP、ICMP等IP层以上的协议的应用，例如即时通讯、视频、语音、Ping等服务；支持PC终端使用包括Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；支持Windows、IOS、Android、塞班、黑莓等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入，或通过PPTP、L2TP VPN方式接入；#支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows EDGE，Google Chrome，Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用； 产品支持国际通用标准的密码算法，包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1等；产品可扩展支持中国国家标准的商用密码算法，包括：SM1，SM2、SM3、SM4。 |
| 应用封装 | ★产品必须支持经过集成的，基于Android IOS平台的第三方软件开发包（SDK）。支持针对移动APP的VPN安全代码的自动封装，实现App应用的安全加固；自动封装后，支持应用图形锁，要求集成安全SDK的企业APP需具备手势认证功能，为企业应用的切换提供快速的二次验证机制，保障企业应用的使用安全； |
| 双域隔离 | 支持在Android、iOS终端上基于沙盒技术生成隔离的安全工作区域，为用户提供安全的办公环境；#安全工作域支持离线登陆，仅验证手势密码即可，保证离线状态下员工可以访问本地应用和数据；安全应用只能从安全域启动，若工作域未登录，从个人桌面、最近运行列表、下拉通知栏等方式启动安全应用时，先调用安全工作域登录认证；#支持对企业应用的文件系统进行安全隔离，使得企业应用和个人应用的存储目录完全隔离，无法相互访问各自的文件；用户切换安全工作域到后台超过一分钟以后，再次切回安全工作域的时候，需要支持手势密码进行身份认证，防止信息泄密；★支持工作域中的原生App单点登录，支持企业APP的单点登录，最终用户通过身份验证、登录到安全隔离区域后，所有企业APP无需再次登录，即可使用，增加易用性，提升办公效率。#支持对企业应用的分享功能进行控制隔离，安全应用的分享功能仅在隔离区域生效，无法将文件和数据分享到个人应用中，保障企业数据安全。#支持对企业应用的剪切板进行控制隔离，禁止在用户从企业应用中复制内容粘贴到个人应用中，防止企业敏感数据泄露。★iOS切换到后台后界面模糊，防止未授权的偷窥导致信息泄漏。 |
| 权限、服务器安全 | 产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的IP地址、端口、提供的服务、URL地址等进行权限控制；针对同一B/S资源，可对不同用户做到细致到URL级别的授权；产品应具有角色授权机制，支持在用户组的基础上，根据角色的不同，组合关联不同的资源权限；★支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统； |
| 身份认证 | 产品必须支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证；支持有驱USB KEY、无驱USB KEY认证，无驱KEY无需在客户端安装驱动，方便用户；设备内部必须支持自建CA中心，便于数字证书认证平台搭建；#单台VPN设备可扩展同时支持5套以上CA根证书； |
| 高速性 | #必须支持至少4条以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠SSLVPN设备同样可实现SSLVPN接入用户的多线路自动优选功能；#支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度；#支持利用网页进行动态寻址的方法，客户端无需安装插件、不依靠IP地址库、不依赖于第三方动态IP寻址、直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（简称Webagent页面），通过Webagent页面自动寻找VPN设备IP(非DDNS),该方法不必单独注册域名或占用IP地址，大大降低了系统部署难度；#支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输；★针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果； |
| 稳定性、可扩展性 | 支持10台不同型号设备间进行集群（A/A），支持路由模式、单臂模式下多线路部署的集群；支持集群设备间Session同步，一台设备宕机后其上用户无需重新登录SSLVPN可继续使用；可扩展分布式集群功能，无需专门的全局负载设备即可实现异地SSLVPN设备间的接入用户负载分担、速度优选接入，异地设备间互为备份，分布式集群中用户可通过唯一的一个地址访问到所有加入到分布式集群的SSLVPN设备；★在负载均衡集群部署模式下，支持授权漂移，即当集群中一台设备宕机，该宕机设备中的并发授权自动迁移到其他正常的设备中，而无需额外购买授权； |

注：投标结束后，采购人将对中标产品进行性能测试和功能验证，与投标承诺不符将做为无效投标处理，由此引发的所有损失由该投标人承担。

第三部分：资质与服务要求

1. 必要资质要求
* 提供厂商针对本项目的授权书和售后服务承诺函；
* 提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》；
* 提供国家版权局颁发的《计算机软件著作权登记证》；
* 厂商具备网络安全应急服务支撑单位证书（国家级）。
1. 非必要资质要求
* 提供产品IPV6 Ready认证证书，并在全球IPV6测试中心官网可查；
* 为保障软件开发质量，厂商需具备CMMI L5认证证书；
1. 服务要求

提供三年原厂免费服务，包括软件升级，硬件质保，现场技术支持服务，电话支持服务。