**南方医科大学口腔医院**

**上网管理相关设备项目建设需求书**

## 项目概述

### 项目背景

目前医院在使用中的上网行为管理及防火墙设备是2017年“银医通”项目中由银行采购，主要用于医院办公外网及患者WIFI的管理和安全防护，随着医院业务的发展和国家网络安全法规的完善，设备的性能已经无法满足医院当下的业务需求及现今的网络安全要求。为了维持医院的互联网边界安全防护能力，现考虑对现有的上网行为管理、防火墙等设备进行替换，新设备需继承原有设备上的策略和数据，并将原有网监备案转移到新设备上。通过新旧设备的替换，实现医院边界安全防护能力的增强，满足《卫生部办公厅关于全面开展卫生行业信息安全等级保护工作的通知》、《中华人民共和国网络安全法》、《网络安全等级保护基本要求》等标准的合规要求，同时能够全方面为医院的业务系统提供持续的安全保护。

### 建设目标

（1）原上网行为管理型号：深信服AC-1000-C600，系统版本：AC13.0.7；

原防火墙型号：深信服AF-1820，系统版本：NGAF 7.4；

原无线控制器型号：H3C WX2510H-F

（2）采购新设备替换现有的上网行为管理、防火墙设备及无线控制器，新设备可以继承原有设备上的策略和数据，实现新旧设备安全能力的平滑过渡和升级，并可以将原有设备上的网监备案转移到新设备上，无线控制器需要支持H3C WA6320和H3C WA6520等原有AP，新设备至少提供3年原厂质保。；

（3）根据医院实际使用情况，新设备可以支持同时在线3000人及以上，新设备接入的互联网线路带宽满足大于等于750Mb，支持同时接入多家运营商的互联网线路，实现多链路访问的流畅性；

（4）新设备满足网络安全等级保护的技术要求中的安全通用要求，包括身份鉴别、访问控制、安全审计、入侵防范等；

### 项目建设内容清单

1.3.1设备建设清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **模块名称** | **数量** | **单位** |
| 1 | 上网行为管理 | 1 | 台 |
| 2 | 下一代防火墙 | 1 | 台 |
| 3 | 无线控制器 | 1 | 台 |

1.3.2服务清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **类别** | **模块名称** | **数量** |
| 1 | 服务 | 设备和软件3年运维及质保服务 | 1套 |
| 2 | 服务 | 原策略、数据和网监备案迁移及新设备软硬件安装调试 | 1项 |
| 3 | 服务 | AP管理授权 | 32个 |

## 技术参数

上网行为管理

|  |  |
| --- | --- |
| **项目** | **功能要求说明** |
| 硬件  要求 | ▲硬件规格≥1U，内存大小≥8G，硬盘容量≥64G SSD+960G SSD，接口不少于6个千兆电口+2个万兆光口SFP+ |
| 性能  要求 | ▲网络层吞吐量≥8Gb，应用层吞吐量≥1.1 Gb，带宽性能≥750Mb，支持用户数≥5000，每秒新建连接数≥12000，最大并发连接数≥50万 |
| 部署  方式 | 支持网关模式、网桥模式、旁路模式部署； |
| ▲支持两台及两台以上设备同时做主机的部署模式； |
| 网监备案要求 | ★本次采购设备可以继承医院已有上网行为管理设备上的策略和数据，实现新旧设备安全能力的平滑过渡和升级，并支持将原有设备上的网监备案转移到新设备上（提供承诺函，格式自拟）； |
| 系统管理 | 多台设备支持通过统一平台集中管理、集中配置等； |
| 认证  方式 | 支持触发式WEB认证，用户名密码认证等； |
| ▲为简化登录流程，要求支持终端用户可以使用账号绑定的手机号码，接收短信验证码，然后使用手机号码和验证码完成密码认证。支持在终端用户的账号存在微信绑定关系的情况下，PC端的终端用户可以直接使用微信扫码二维码完成密码认证过程，移动端的终端用户，可以直接打开微信扫码完成密码认证过程。（提供产品界面截图并加盖厂家公章） |
| 支持绑定IP认证、绑定MAC认证，及IP/MAC绑定认证等，支持通过SNMP服务器跨三层获取MAC地址； |
| 密码登录支持用户自注册，通过Web页面申请注册新账号，管理员审批后新账号可用；（提供产品界面截图并加盖厂家公章） |
| ▲支持通过OAuth认证协议对接，支持阿里钉钉，企业微信第三方账号授权认证；（提供产品界面截图并加盖厂家公章） |
| 功能  要求 | ▲设备内置海量预分类的URL地址库，能够针对：网上购物、成人内容、求职招聘、宗教、在线影音及下载、游戏资讯、网上聊天、个人网站及博客、色情、赌博、非法药物、风水命理、娱乐场所、汽车、餐饮、钓鱼及恶意网站、网上银行、在线支付等各种URL类型做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制。（提供产品界面截图并加盖厂家公章） |
| ▲设备内置应用识别规则库，支持超过10000条应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并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；（提供产品界面截图并加盖厂家公章） |
| ▲支持Teamviewer、向日葵、Anydesk、RDP的远程应用的外发文件审计；（提供产品界面截图并加盖厂家公章） |
| 资质  要求 | 应为市场成熟产品，最近两年在国内IDC内容安全市场占有率排名都在前三，提供相应证明材料截图 |
| 产品应具备相当的技术认可度，产品曾连续两年入围Gartner SWG魔力象限，提供相应证明材料截图 |

下一代防火墙

|  |  |
| --- | --- |
| **指标** | **功能要求说明** |
| 硬件  要求 | 硬件规格≥2U，内存大小≥8G，硬盘容量≥64G SSD+480G SSD，冗余电源，接口不少于16个千兆电口+2个千兆光口+4个万兆光口SFP+ |
| 性能  要求 | ▲网络层吞吐量≥15Gbps，应用层吞吐量≥6Gbps，防病毒吞吐量≥1 Gbps，IPS吞吐量≥1Gbps，全威胁吞吐量≥800M,并发连接数≥200万，每秒新建连接数≥9万。 |
| 网络适应性 | 产品支持静态路由、策略路由、多播路由等常见路由类型。 |
| 产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。 |
| 产品支持IPsec VPN和SSL VPN功能。 |
| ▲产品支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换。（提供产品界面截图并加盖厂家公章） |
| 产品支持IPSecVPN链路优化功能，在高丢包场景下，依然保障业务流畅访问体验。 |
| 应用  控制 | ▲产品支持应用管控功能，支持对应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等进行检测与控制，应用特征识别库数量大于9000种。（提供产品界面截图并加盖厂家公章） |
| 访问  控制 | 产品支持基于网络区域、网络对象、MAC地址、服务、应用等维度进行访问控制策略设置。 |
| ▲产品支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。（提供产品界面截图并加盖厂家公章） |
| 产品支持杀毒白名单设置，可以例外排除特定MD5和URL的病毒文件，针对特定文件不进行查杀。 |
| ▲产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略，需提供产品相关功能截图，并提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局之中任意一家检测机构出具关于“勒索病毒”的相关证书证明功能有效性。 |
| ▲产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。（提供第三方检测报告并加盖厂家公章） |
| 产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。 |
| ▲产品支持用户账号安全保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。需提供产品相关功能截图，并提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局之中任意一家检测机构出具关于“账号保护”的相关证书证明功能有效性。 |
| 设备  联动 | ▲能够与本次采购的上网行为管理设备实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；（提供产品界面截图并加盖厂家公章） |
| 产品支持主动防御功能，通过与云端蜜罐智能联动，通过仿真虚拟业务混淆黑客攻击，并对攻击进行溯源取证和阻断威胁IP，保护网络真实业务安全。需提供产品功能截图证明，并提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局之中任意一家检测机构出具关于“主动防御”的相关证书证明功能有效性。 |
| 服务 | ▲支持包括WEB应用防护识别库、IPS特征库、僵尸网络防护库、实时漏洞分析识别库和URL&应用识别库定期更新服务不少于3年，保持设备具备检测防御最新威胁的能力。 |
| 资质  要求 | 要求所投产品具备计算机信息系统安全专用产品销售许可证，提供有效证书复印件。 |
| 要求所投产品具备中国国家信息安全产品认证证书，提供有效证书复印件。 |
|  | 要求所投产品具备IT产品信息安全认证证书EAL4增强级，提供有效证书复印件。 |
|  | 要求防火墙所投产品的生产厂商参与制定《信息安全技术 第二代防火墙安全技术 要求》，需提供证明材料。 |

无线控制器

|  |  |
| --- | --- |
| **指标** | **功能要求说明** |
| 管理  AP数 | 支持常规AP最大数量≥128，含32个AP管理授权 |
| 端口  要求 | LAN:6\*GE  WAN:2\*GE  10GBASE-R-SFP+口2个  USB≥1个 |
| 转发  性能 | 集中转发性能≥4Gbps |
| 组网  能力 | 支持标准IETF 5415 CAPWAP协议，AP和AC之间支持L2/L3层网络拓扑，为提高网络安全，AP与控制器之间能够支持DTLS对CAPWAP隧道进行加密处理。 |
| 认证  加密 | 支持MAC 地址认证、802.1x认证（EAP-PAP、EAP-MD5、EAP-PEAP、EAP-TLS、EAP-TTLS）、Portal认证、MAC+Portal混合认证；  支持WPA标准、WEP(WEP64/WEP128)、TKIP、CCMP；  支持内置portal、dot1x服务器；  支持Private PSK方式的动态密码功能，可以为每终端分配独立秘钥。  支持WPA3个人级方式下的终端接入；支持WPA3企业级模式下的终端接入功能。  支持防PSK暴力破解，当用户密码错误超过预设的阀值之后，能够将该用户加入动态黑名单，一段时间内禁止其接入网络 |
| 无线  漫游 | 支持AC内漫游，支持跨AC间漫游，支持跨VLAN的三层漫游  支持基于802.11k/802.11v/802.11r协议的智能漫游 |
| 可靠性 | 支持雷达检测SSID逃生功能：AC、AP支持SSID自主逃生，当AP射频检测到雷达信号时，会将本射频的SSID迁移到其他射频，保障关键业务正常通信。  MAC认证逃生功能：AC、AP支持MAC认证逃生功能，为提高无线网络认证可靠性，无线控制器支持MAC认证逃生功能。  支持Dot1x认证逃生功能：AC、AP支持Dot1x认证逃生功能，为提高无线网络认证可靠性，无线控制器支持Dot1x认证逃生功能。  支持Portal认证逃生功能：AC、AP支持Portal认证逃生，为提高无线网络认证可靠性，无线控制器支持Portal认证逃生功能。  支持RemoteAP功能：AC、AP支持RemoteAP功能，为提升无线网络的可靠性，AP具备逃生功能，当AC不可达造成AP离线时，AP能够继续维持原有用户不下线，新用户仍可以接入网络保证业务正常。支持认证用户和非认证用户。 |
| 认证  加密 | 支持Portal在线用户与DHCP租约联动功能：AC支持根据DHCP租约信息联动Portal用户自动下线，可以提高DHCP地址池的利用率，降低Portal重复认证开销。  能够有效拦截Portal用户重定向攻击 |
| 无线  运维 | 为监控AP有线端口异常所引起的无线网络体检较差的原因，所投产品需要支持：有线端口接收错包持续增长、AP有线端口Down、有线端口协商速率低、有线端口发送错包持续增加、有线端口协商成半双工等问题的检测，需要提供功能截图证明  ▲为实现AC的全面运维，所投产品需要支持：AC CPU、内存使用率以及历史信息，AC整机广播、组播、单播流量成分以及历史信息，AC仿真面板端口图以及每端口广播、组播、单播流量成分以及历史信息，同时可以识别最近一分钟端口入方向广播组播占比过高、最近一分钟端口流量过大等异常事件，需要提供第三方认证报告证明  为保障重要用户的无线网络体验，所投产品需要支持VIP功能，并图形化展示VIP用户速率、延时、平均信号强度等无线体验信息，要求提供截图证明  为使得网络管理员实时感知网络状态，所投产品需要在网络发生异常时，可利用短信、微信、邮件等三种不同方式推送告警信息，要求提第三方认证报告证明  为了保障无线网络的用户体验，所投产品需要支持对弱信号接入、乒乓漫游等常见无线网络问题的识别，并给出问题分布趋势图、该问题所影响的具体终端、涉及的AP以及该AP发生该异常的数量统计，需要提供第三方认证报告证明。 |
| 进网许可证 | ▲要求提供所投设备进网许可证 |
| CCC认证报告 | ▲要求提供国家强制性产品认证证书 |

备注：凡标有“★”的地方均为实质性响应条款，供应商若有一项带“★”的条款未响应或不满足，将按无效响应处理；“▲”为重要条款。

## 售后服务要求

1. 供应商应有良好的服务理念和完善的售后服务体系，能够提供本地技术服务。
2. 质保期：三年。
3. 针对本项目，提出完整而切实可行的服务方案，提供7×24小时热线电话、远程网络、现场等服务方式。
4. 供应履约过程中，必须遵守国家有关法律的规定，如实提供检查所必须的材料，不得拒绝。

四、供应商资格要求

(1)在中华人民共和国境内注册的具有独立承担民事责任能力的法人或其他组织；

(2)提供履行合同所必需的设备和专业技术能力的书面声明，提供本地化服务。（供应商出具声明函）；

(3)单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的采购活动。（供应商出具声明函）；

(4)供应商未被列入“信用中国”网站(www.creditchina.gov.cn) 以下任何记录名单之一：①失信被执行人；②重大税收违法案件当事人名单。

(5)供应商需要具备质量管理体系认证证书。