## 项目概况

2011年12月，卫生部发布《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》, 要求卫生行业“全面开展信息安全等级保护工作”，《中华人民共和国网络安全法》自2017年6月1日开始施行。其中，《网络安全法》第21条明确规定了“国家实行网络安全等级保护制度”。2019年5月13日，国家标准化管理委员会发布了新修订的《信息安全技术-网络安全等级保护基本要求》，即“等保2.0”标准正式开始施行。国家各级层面都非常重视网络安全工作。
 我院信息系统的安全性直接关系到医院医疗工作的正常运行，一旦发生故障或数据丢失，将给医院和社会带来巨大的灾难和难以弥补的损失。近年来，网络安全事件频发，很多单位受到网络安全攻击事件的威胁。一旦发生网络安全事件，将对医院的正常工作开展产生巨大影响，造成不可估量的损失。必须要加强网络安全防护建设。我院吸取其他医院的教训，有必要对医院的网络安全工作进行梳理，加强网络安全建设，防止发生类似安全事件。

依照《中华人民共和国网络安全法》、《国家信息化发展战略纲要》、《网络安全等级保护基本要求》(GB/T 22239-2019)等要求，进一步加大网络安全平台建设投入，提升与完善医院网络与信息安全水平。我院之前做了安全防护的项目，堡垒机产品授权不够需要扩容，网闸是单机部署存在单点故障，上网行为管理已经使用8年多，设备老化、性能不足，需要更换更高性能设备。增加动态WAF设备，防止未知漏洞攻击，主要是对以前安全建设的补充和更新，使我院的网络安全建设既可以满足等级保护的相关要求，又能够全方面为业务系统提供立体、纵深的安全保障防御体系，保证信息系统整体的安全保护能力。

## 一、项目软硬件配置数量、价格及预算清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目** | **推荐品牌** | **配置参数** | **数量** | **单位** |
| 1 | 上网行为管理 | 深信服、启明星辰、华三 | 网络层吞吐量（大包）：4.8Gb，应用层吞吐量：600Mb，带宽性能：400Mb，IPSEC VPN加密性能（最高性能）：120Mb，支持用户数：3000，包转发率：72Kpps，每秒新建连接数：8000，最大并发连接数：400000。规格：1U，内存大小：4G，硬盘容量：1T SATA，电源：单电源，接口：4千兆电口+4千兆光口SFP。三年质保、三年软件升级、三年URL规则库升级 | 1 | 台 |
| 2 | 服务器EDR | 深信服、启明星辰、华三 | 针对Windwos Server操作系统进行病毒查杀，提供主动防御系统防护,补丁管理功能，支持对全网终端系统漏洞发现、补丁智能修复、强制修复等、蓝屏修复、补丁分发流量控制、客户端P2P补丁分发加速等功能。系统默认支持WIN2003/WIN2008/WIN2012/，含三年升级服务。 | 40 | 用户 |
| 针对linux服务器操作系统进行病毒查杀，智防服务器模块包含：通用特征检测：提供已知威胁检测能力；人工智能检测：无特征检测技术，提供未知威胁检测能力；文件实时监控：支持文件实时监控扫描、威胁自动处置，漏洞检测及修复；智响应客户端模块包含： 智能联动响应，支持威胁情报共享与自动响应功能； 全网威胁定位：提供基于威胁情报的全网威胁搜索定位以及隔离处置功能；含三年升级维护费用。 | 30 | 用户 |
| 3 | 内外网互连防火墙 | 深信服、启明星辰、华三 | 网络层吞吐量：6G，应用层吞吐量：2G，防病毒吞吐量：800M，IPS吞吐量：500M，全威胁吞吐量：400M，并发连接数：180万，HTTP新建连接数：6万，规格：1U，内存大小：4G，硬盘容量：64G minisata SSD，电源：单电源，接口：6千兆电口+4千兆光口SFP。开通增强级，三年质保，三年软件升级，三年安全规则库。 | 1 | 台 |
| 4 | 卫生平台专线防火墙 | 深信服、启明星辰、华三 | 网络层吞吐量：3G，应用层吞吐量：600M，IPS吞吐量：150M，防病毒吞吐量：250M，全威胁吞吐量：130M，并发连接数：80万，HTTP新建连接数：1.8万，规格：1U，内存大小：2G，硬盘容量：64G minisata SSD，电源：单电源，接口：6千兆电口。三年质保，三年软件升级，三年安全规则库。 | 1 | 台 |
| 5 | 网闸 | 深信服、启明星辰、杭州合众 | 2U机架式、性能要求：吞吐不少于950Mbps；并发不少于6万；延时小于1ms。内网接口：不少于1个console口、3个10M/100M/1000M电口（其中包含一个管理口、1个HA口）、2个USB口，管理口与业务口相互独立。可扩展至6个10M/100M/1000M电口。原厂三年质保及升级。 | 1 | 台 |
| 6 | 动态WAF | 深信服、启明星辰、瑞数 | 400MB，1个 虚拟机许可， 4C，16G，含操作系统和三年标准服务通过部署动态应用防护系统，可以带来如下收益：l 网站漏洞隐藏：使漏洞扫描、漏洞利用工具、零日漏洞探测工具无法发起有效攻击，在网站未打补丁和补丁空窗期提供有效安全保护。l 传统应用安全威胁防护：有效防止传统WAF能防护的各类常规注入类攻击。l 自动化攻击防护：有效防护攻击者利用自动化攻击脚本或工具对应用发起的攻击行为。l 模拟合法操作防护：有效应对攻击者利用工具、合法身份，模拟正常人工访问的攻击行为。l 数据防泄漏：有效防护恶意人员使用工具或脚本程序通过前台应用批量获取数据的攻击行为。 | 1 | 套 |
| 7 | 堡垒机扩容 | 原有品牌：齐治堡垒机 | 堡垒机授权增加100管理授权 | 1 | 项 |

## 二、技术要求

**1、上网行为管理**

|  |  |
| --- | --- |
| 项目 | 参数要求 |
| 性能要求 | 网络吞吐量≥4.8Gb，并发会话数≥400000，用户规模≥3000人，硬盘≥1TB |
| 设备接口 | 千兆电口≥4个，千兆光口≥4个，支持ByPass，单电源，1U标准机架式设备 |
| 部署方式 | 支持网关模式，网桥模式，旁路模式和多路桥接等多种部署模式 |
| 支持两台及两台以上设备同时做主机的部署模式 |
| 支持部署在IPv6环境中，且其所有功能（认证、应用控制、流量控制、内容审计、报表等）都支持IPv6 |
| 网关管理 | 支持SSL加密WEB方式、SSH命令行方式管理设备 |
| 支持细致的管理员权限划分，包括对不同用户组的管理权限、对各种主要功能界面的配置和查看权限 |
| IPSec支持硬件特征码绑定认证 |
| 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 |
| 实时监控 | 提供设备实时CPU、内存、磁盘占有率、在线用户数、系统时间、网络接口等信息 |
| 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 |
| 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； |
| 认证方式 | 第三方认证：支持触发式WEB认证，静态用户名密码认证等 |
| USB-KEY双因素认证：支持以USB-Key方式实现双因素身份认证 |
| IP、MAC认证：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；支持当用户MAC地址变动时，需要重新认证； |
| 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。 |
| 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； |
| 应用管理 | 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 |
| 1. 设备内置应用识别规则库，支持超过6000条应用规则数，支持超过2800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；

2.支持根据IP、端口、协议等自定义应用规则；3.支持根据不同的应用类型或具体的某种应用设置允许或拒绝； |
| 1.不允许使用外部HTTP代理；2.不允许使用外部Sock4/5代理；3.不允许在HTTP,SSL一些的标准端口上使用其他协议；（比如在80端口上传输非HTTP协议数据，在443端口上传输非HTTPS协议数据等） |
| 能够对平时使用的应用软件最细分控制，登录、浏览、发微博、上传附件等。 |
| 网页管理 | 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;  |
| 识别并过滤SSL加密的钓鱼网站、非法网站等，必须支持https网页全解密和按网站类别分类进行解密配置；  |
| 设备支持管理者自定义新的URL地址和URL分类 |
| 支持基于关键字过滤SSL加密的网页、论坛、BBS上的发帖行为； |
| 支持根据文件类型限制http、FTP方式上传、下载行为； |
| 上网权限与流量控制 | 支持统计和控制用户终端每天上网时间，并支持排除应用或特殊端口后的灵活流量统计方法 |
| 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 |
| 支持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。 |
| 支持根据源地址和目的地址过滤外发邮件；必须支持https网页全解密和按网站类别分类进行解密配置； |
| 支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率 |
| 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；  |
| 支持对加密HTTPS、SMTP-SSL、SMTP的邮件进行关键字过滤，必须能够基于关键字识别和过滤使用SSL加密的Webmail邮箱外发邮件的行为，比如QQ邮箱；  |
| 上网行为审计 | 支持审计用户的明文发帖内容，能审计用户在SSL加密论坛、BBS上的发帖内容； |
| 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 |
| 支持根据QQ、微信账号查询IM聊天行为和内容； |
| 支持对加密HTTPS、POP3-SSL 、POP3、IMAP 、IMAP-SSL、SMTP-SSL、SMTP邮件内容的审计； |
| 上网日志管理及排障处理 | 支持查询和导出基于指定时间段/用户/用户组的文件审计、邮件收发、访问网站、即时通讯、发帖/微博、搜索关键字等详细用户行为的报表 |
| 支持基于时间段/用户/用户组/终端类型/位置等维度的应用流量排行、网站分类流量排行 |
| 支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略； |
| 产品资质 | 具备公安部颁发的销售许可证 |
| 测试 | 要求中标候选人在3个工作日内提供测试设备。通过对招标要求项逐一对比测试，如经设备测试发现与标书要求或投标文件不一致或中标候选人有意拖延测试，将视为虚假应标。 |

**2、服务器EDR**

|  |  |
| --- | --- |
| 项目 | 参数要求 |
| Windows 服务器客户端支持 | Windows Server 2003 SP2/Windows Server 2008/Windows Server 2008 R2/Windows Server 2012/Windows Server 2016 |
| Linux 服务器 客户端支持 | CentOS/UbuntuDebian/RHEL/SUSE/Red Flag Asianux Server/Oracle Linux |
| Windows PC 客户端支持 | Windows XP sp3/Windows Vista/Windows 7/Windows 8/Windows 8.1/Windows 10 |
| 终端安全可视 | 采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能 |
| 支持显示当前未处理的病毒数量、勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量 |
| 支持展示全球热点风险事件在网内终端的爆发情况，及时了解、处置网内终端的热点风险事件，并显示影响终端数量 |
| 终端管理 | 支持展示终端资产状况，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端agent版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新；  |
| 支持以安全策略模板方式对指定终端组快速部署安全策略，安全策略模板支持默认模板和自定义模板； |
| 支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell检测的检测和威胁处置方式、暴力破解的威胁处置方式和信任目录； |
| 终端威胁视角 | 支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析（客户情况、影响行业、区域分布）、威胁分析和处理建议等 |
| 终端风险报表 | 支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议 |
| 邮件告警 | 支持针对管理控制中心性能，安全事件，勒索病毒事件等邮件告警 |
| 错峰升级 | 支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O风暴； |
| 管理员管理 | 支持配置不同的权限角色，支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限 |
| 具备基于人工智能的检测引擎，具备无特征检测技术，有效应对恶意代码及其变种 |
| 防病毒模块 | 具备基于本地缓存信誉检测与全网信誉检测，构建企业全网信誉库的检测引擎，做到企业内网一台威胁，全网感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置有效提升查杀效率，减少终端资源开销 |
| 具备基于虚拟沙盒、引擎和操作系统环境仿真的检测引擎，通过分析多维构成的行为有效识别威胁 |
| 支持本地查杀缓存，具备二级缓存机制：终端侧使用全盘文件缓存，加速本地二次扫描速度，减少对本地虚拟化环境的资源消耗；管理平台侧使用全网文件缓存，加速云查杀速度，减少通过互联网进行云查杀的带宽消耗。 |
| 支持对常见压缩文件的查杀，支持压缩文件查杀层级进行策略配置，最大可配置检查10层压缩文件； |
| 支持agent安装目录的文件保护，可以保护agent目录和文件实时监控驱动文件，可以保护agent的服务/进程/文件不被恶意删除，影响正常功能，导致用户的终端受到病毒入侵 |
| 支持对来自Internet、E-mail或是光盘、移动存储、网络等各种入口渠道病毒进行实时检测 |
| 构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置 |
| 一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果 |
| 智能控制模块 | 提供对业务系统之间、业务系统内不同应用角色之间、业务系统内相同应用角色之间的访问控制策略配置 |
| 支持微隔离功能主界面图形化显示业务系统、服务器及流量详情；  |
| 流量线详情支持展示该流量线对应的微隔离策略；图形化显示服务器间流量关系，包括访问详情、流量趋势等； |
| 支持管理平台向终端下发脚本（.bat和.sh）执行文件，方便管理人员对终端进行脚本下发 |
| 联动响应模块 | 支持基于威胁情报的病毒特征值全网终端搜索，可定位出全网终端该病毒的感染情况 |
| 支持管理员在同厂商的安全感知平台管理界面下发快速查杀任务，并查看任务状态，结果并进行处置 |
| 支持管理员在同厂商的安全感知平台管理界面下发一键隔离指令，对终端所有连接进行阻断，防止病毒进一步扩散 |
| 支持将终端安全软件客户端检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到同厂商安全态势感知平台，安全态势感知平台进行分析和展示； |
| 产品资质 | 提供公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》资质证书 |
| 测试 | 要求中标候选人在3个工作日内提供测试设备。通过对招标要求项逐一对比测试，如经设备测试发现与标书要求或投标文件不一致或中标候选人有意拖延测试，将视为虚假应标。 |

**3、内外网互连防火墙**

|  |  |
| --- | --- |
| 项目 | 参数要求 |
| 性能要求 | 三层吞吐量≥6G，应用层吞吐量≥2G，并发连接数≥180万，每秒新建连接≥6万/秒， |
| 设备接口 | 千兆电口≥6个，千兆光口≥4个，1U标准架构，单电源 |
| 部署方式 | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式 |
| 网络特性 | 支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口 |
| 支持链路聚合功能 |
| 支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路 |
| 支持IPV6环境部署，包括接口/区域配置、路由配置等网络适应性功能，支持核心常用安全功能，包括僵尸网络，IPS漏洞防御，WEB应用防护等，支持协议一致性（包括但不限于Core、NDP、Autoconfig、PMTU、ICMPV6）和协议健壮性检测（IPv6畸形报文、ICMPv6畸形报文、其他协议畸形报文），支持IPV6的地址转换、双栈的过渡技术 |
| 路由支持 | 支持静态路由，ECMP等价路由以及RIPv1/v2，OSPFv2/v3，BGP等动态路由协议 |
| 支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能 |
| 基础功能 | 支持连接会话展示，可针对具体的IP地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体IP的会话记录 |
| 访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试 |
| 支持根据国家/地区来进行地域访问控制 |
| 支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式； |
| DoS/DDoS攻击防护 | 支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 |
| 支持TearDrop 攻击、IP数据块分片传输、Land攻击、Smurf攻击、WinNuke攻击、超大ICMP数据攻击等异常报文攻击防护，支持IP协议异常报文和TCP协议异常报文攻击防护。 |
| 支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为 |
| 入侵防护功能 | 设备具备独立的入侵防护漏洞规则特征库，特征总数在7400条以上 |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telne、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能 |
| 具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。 |
| 具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能 |
| 安全策略管理 | 支持针对业务攻击事件汇总，展示攻击事件类型TOP5及当前业务命中的全网实时热点事件，支持通过地图区域颜色深浅展示攻击者的分布与数量。 |
| 支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。 |
| 安全可视化 | 支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别 |
| 支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险；  |
| 支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证 |
| 产品资质 | 产品应具备计算机信息系统安全专用产品销售许可证 |
| 测试 | 要求中标候选人在3个工作日内提供测试设备。通过对招标要求项逐一对比测试，如经设备测试发现与标书要求或投标文件不一致或中标候选人有意拖延测试，将视为虚假应标。 |

**4、卫生平台专线防火墙**

|  |  |
| --- | --- |
| 项目 | 参数要求 |
| 性能要求 | 三层吞吐量≥3G，应用层吞吐量≥600M，并发连接数≥80万，每秒新建连接≥1.8万/秒， |
| 设备接口 | 千兆电口≥6个，1U标准架构，单电源 |
| 部署方式 | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式 |
| 网络特性 | 支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口 |
| 支持链路聚合功能 |
| 支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路 |
| 支持IPV6环境部署，包括接口/区域配置、路由配置等网络适应性功能，支持核心常用安全功能，包括僵尸网络，IPS漏洞防御，WEB应用防护等，支持协议一致性（包括但不限于Core、NDP、Autoconfig、PMTU、ICMPV6）和协议健壮性检测（IPv6畸形报文、ICMPv6畸形报文、其他协议畸形报文），支持IPV6的地址转换、双栈的过渡技术 |
| 路由支持 | 支持静态路由，ECMP等价路由以及RIPv1/v2，OSPFv2/v3，BGP等动态路由协议 |
| 支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能 |
| 基础功能 | 支持连接会话展示，可针对具体的IP地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体IP的会话记录 |
| 访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试 |
| 支持根据国家/地区来进行地域访问控制 |
| 支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式； |
| DoS/DDoS攻击防护 | 支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 |
| 支持TearDrop 攻击、IP数据块分片传输、Land攻击、Smurf攻击、WinNuke攻击、超大ICMP数据攻击等异常报文攻击防护，支持IP协议异常报文和TCP协议异常报文攻击防护。 |
| 支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为 |
| 入侵防护功能 | 设备具备独立的入侵防护漏洞规则特征库，特征总数在7400条以上 |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telne、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能 |
| 具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。 |
| 具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能 |
| 安全策略管理 | 支持针对业务攻击事件汇总，展示攻击事件类型TOP5及当前业务命中的全网实时热点事件，支持通过地图区域颜色深浅展示攻击者的分布与数量。 |
| 支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。 |
| 安全可视化 | 支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别 |
| 支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险；  |
| 支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证 |
| 产品资质 | 产品应具备计算机信息系统安全专用产品销售许可证 |
| 测试 | 要求中标候选人在3个工作日内提供测试设备。通过对招标要求项逐一对比测试，如经设备测试发现与标书要求或投标文件不一致或中标候选人有意拖延测试，将视为虚假应标。 |

**5、网闸**

|  |  |
| --- | --- |
| 项目 | 参数要求 |
| 接口要求 | 标准2U机架设备。内网接口：不少于1个CONSOLE口、设备标配6个10/100/1000M和2个SFP插槽、2个USB口。外网接口：不少于1个CONSOLE口、设备标配6个10/100/1000M和2个SFP插槽、2个USB口。 |
| 硬件要求 | 设备提供“健康指示灯”提供声音报警装置。设备处于异常状态下，能通过指示灯报警，且能通过报警装置发出声音报警。 |
| 性能要求 | 吞吐量≧950Mbps；并发≧6万；延时小于1ms。 |
| 系统架构 | 采用“2+1”系统架构，即由两个主机系统和一个隔离交换专用硬件组成；隔离交换矩阵基于专用芯片实现，保证数据在搬移的时间内，内、外网隔离卡与内、外网系统为断开状态。 |
| 系统要求 | 内外网主机系统分别支持双系统引导，并可在WEB界面上直接配置启动顺序，在A系统发生故障时，可以随时切换到B系统；且支持系统(包括配置)备份；  |
| IPv6环境支持 | 支持纯IPv6网络环境，能够在纯IPv6网络环境下正常工作 |
| 强制访问控制 | 支持WEB认证方式和专用客户端两种认证方式； |
| 可对用户的客户端版本和进程进行检查，进行准入控制； |
| 文件同步 | 支持NFS、SMBFS等文件系统；文件服务器可以是Windows、Linux/Unix等系统平台； |
| 支持文件传输方向可控，实现单向或双向传输； |
| 支持文件格式特征过滤；并能提供文件类型判断工具以帮助用户识别不常见文件类型 |
| 重名策略，接收端客户端支持对重名文件的控制策略，提供“覆盖”、“丢弃”、“重命名”等重名策略。 |
| 可根据异常条件进行报警，如MD5校验失败、堆内存占用过高等条件支持邮件报警方式； |
| 数据库同步 | 支持Oracle、SQL Server、Sybase、Db2、MySQL等主流数据库；数据库同步客户端支持Windows、Linux等主流平台； |
| 支持同种数据库间（同构）和不同种数据库间（异构）的同步； |
| 支持灵活的数据库冲突处理策略，当关键字数据发生冲突时可选择：覆盖/丢弃；  |
| 支持数据库同步客户端的双机热备技术，为用户提供更高的冗余技术支持；  |
| 支持数据容错处理，当数据同步失败时，用户可以查询、恢复、删除未能正常传输的数据。 |
| 支持客户端与网闸间的数字证书方式的身份认证；  |
| 数据库传输 | 实现对多种（如MySql、SqlServer、Oracle、DB2、Sybase）主流数据库系统的安全访问； |
| 提供数据库访问用户的过滤和控制； |
| 支持数据库SQL语句过滤功能。 |
| 支持用户身份认证 |
| FTP访问 | 实现安全的FTP访问，支持对访问用户、访问协议命令、上传下载文件类型等访问过滤控制； |
| 支持访问时段策略；时间可以设置为一次性或者周循环方式 |
| 支持用户身份认证 |
| 邮件传输 | 支持基于SMTP协议的邮件发送和POP3协议的邮件接收； |
| 支持邮件主题及正文的关键字过滤，以及收件人、发件人地址黑白名单 |
| 支持对邮件附件大小进行控制；支持附件类型过滤； |
| 邮件收发支持时段访问控制；时间段可以是一次性执行、周循环两种方式 |
| 支持用户身份认证 |
| 安全浏览 | 支持访问源地址、目的地址、目的端口的访问控制； |
| 支持页面关键字过滤，支持MIME类型过滤； |
| 支持网页下载文件类型过滤；支持URL过滤； |
| 支持上网时段控制策略，时间策略可以是一次性或者周循环模式； |
| 支持用户身份认证 |
| 支持HTTP请求头部大小限制 |
| 定制访问 | 实现特定TCP、UDP协议的数据隔离交换，可合作定制开发针对特定协议的安全检测，实现如黑白名单控制、关键字过滤等 |
| 支持源地址、目的地址、目的端口的访问控制。 |
| 支持用户身份认证 |
| 安全通道 | 支持HTTP/HTTPS/FTP/SMTP/POP3等应用协议; |
| 支持H323/H323\_GK等多媒体协议； |
| 支持多种访问控制，比如IP地址和端口访问控制，连续端口范围控制等； |
| 支持时间策略访问控制。 |
| 支持SYN、UDP FLOOD阈值设置 |
| 安全管理 | 支持HTTPS的Web方式管理，实现了远程管理信息加密传输； |
| 内/外网主机系统分别具备独立管理接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网唯一管理接口完成全部管理等； |
| 支持配置文件以加密的方式导出 |
| 双机热备 | 通过独立的热备接口实现双机热备； |
| 支持抢占模式；  |
| 支持配置同步；  |
| 支持与我单位原有网闸进行双机部署，支持主、备状态实时展示； |
| 日志审计与状态监控 | 支持中文日志显示，并能实现内外网主机日志同步 |
| 支持FTP方式上传日志； |
| 支持SNMP v1、v2、v3版本，并支持trap方式。 |
| 提供在线用户状态监控，能够对在线用户列表及在线用户时长进行统计 |
| 产品资质 | 产品具备公安部《计算机信息系统安全专用产品销售许可证》 |
| 测试 | 要求中标候选人在3个工作日内提供测试设备。通过对招标要求项逐一对比测试，如经设备测试发现与标书要求或投标文件不一致或中标候选人有意拖延测试，将视为虚假应标。 |

**6、动态WAF**

|  |  |
| --- | --- |
| 项目 | 参数要求 |
| 部署方式 | 部署架构：透明部署，或反向代理； |
| 部署简单：服务端应用无需更改代码、客户端浏览器无需安装任何插件； |
| 数据存储：支持私有化部署，无需连接云端； |
| 系统升级：支持使用补丁包在线升级，整个过程无需重启系统； |
| 威胁防护 | 自动化漏洞扫描：通过对可攻击点的动态隐藏，自动化工具无法获得攻击入口，可有效防止各类已知与未知漏洞的自动化扫描工具；  |
| 自动化撞库和暴力破解：可防止攻击者通过自动化程序，发起撞库攻击或者暴力破解、猜测敏感数据；  |
| 自动化模拟操作：可防止攻击者通过自动化模拟操作，进行批量建立虚假帐号、盗用帐号、交易欺诈、操纵评价或其它恶意操作行为；  |
| 动态验证：浏览器真实性检测：能识别用户是否使用真实客户端浏览器，包括但不限于扫描器及其他高级自动化工具；  |
| 动态令牌：通过对当前访问页面内的合法请求授予在一定时间内有效的，可防止攻击者发出非法请求，有效抵御越权访问、网页后门及重放攻击等恶意行为；管理员不需要手动配置策略指定需要保护的参数，以降低配置的复杂度和避免可能的安全隐患； |
| 白名单功能 | 请求白名单：对指定的请求页面不检查动态令牌，通常用于静态资源或指定入口； |
| IP白名单：对于指定的来源IP地址进行透传； |
| 日志功能 | 安全日志：包含防护日志、操作审计日志及系统日志； |
| 过滤日志：包含时间、访问网址、来源IP地址、过滤规则及规则细节等； |
| 日志导出：可通过TCP或UDP协议，将日志输出到指定的Syslog服务器； |
| 日志管理：可自动化对日志进行归档及磁盘空间管理； |
| 报表功能 | 支持报表功能 |
| 测试 | 要求中标候选人在3个工作日内提供测试设备。通过对招标要求项逐一对比测试，如经设备测试发现与标书要求或投标文件不一致或中标候选人有意拖延测试，将视为虚假应标。 |

## 三、供应商资格要求

1、供应商须具有具有ISO20000信息技术服务管理体系证书

2、供应商须具有ISO27001信息安全管理体系证书

3、供应商须具有CCRC信息安全服务资质证书（信息系统安全集成）

4、供应商须具有ITSS信息技术服务标准符合性资质证书

5、供应商须具有三年内（2018年1月1日起，以合同签订时间为准）针对医院网络安全多产品集成项目案例（合同中涉及网络安全设备的金额比例不低于80%）