# 苏北人民医院信息安全设备采购技术参数要求

**一、设备采购一览表：**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **数量** | **推荐品牌** |
| 1 | 数据中心防火墙 | 2 | 山石网科、亚信、汉领 |
| 2 | 态势感知平台 | 1 | 山石网科、亚信、绿盟 |
| 3 | 数据库审计平台 | 1 | 山石网科、亚信、汉领 |
| 4 | 边界防毒墙 | 1 | 山石网科、亚信、绿盟 |
| 5 | 集成服务 | 1 | 无 |

**二、技术参数要求（带★号为必须满足项）：**

## 1.数据中心防火墙（2台）

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| **硬件规格** | 硬件平台采用先进的多核网络专用架构。硬件平台采用多核处理器，使用64位MIPS多核处理器；配置冗余双电源。 |
| ★标配4个通用扩展槽位，配置4个10/100/1000MBase-T电口（含一对Bypass接口），4个千兆SFP光纤插槽，2个万兆SFP光纤插槽，至少可扩展至40个千兆接口或者10个万兆接口，每个接口可划分到不同安全域实现各接口间的安全隔离，提供独立的带外管理接口和HA接口。（配置2个万兆多模光模块） |
| 防雷击，必须通过国家无线电监测中心检测中心浪涌（冲击）抗扰度（4KV）测试项目，并出具国家无线电监测中心检测中心委托测试报告 |
| **性能** | ★防火墙性能吞吐率(bps)≥20G，最大并发连接数≥1000万，VPN吞吐量(bps) ≥12G，每秒新建连接数≥30万，IPS吞吐量≥7Gbps，提供IPSec VPN隧道数≥20000条，并发SSL VPN用户许可≥6个； |
| **网络适应性** | 支持BFD 功能，支持BFD与静态路由/OSPF/BGP进行联动。快速检测到与相邻设备间的通信故障，减小设备故障对业务的影响。通过与动态路由协议联动，缩短收敛时间，提升可靠性。 |
| 支持基于源地址、目的地址、生效时间、应用协议（http、https、mysql、ms-sql、sqlnet、sip等）限制新建连接、并发连接； |
| 支持基于应用协议的路由功能，根据应用类型进行路由选择。 |
| ★支持线路过载保护功能，当某条外网线路拥塞时，自动将其流量切换到其他链路；系统对各出口的流量带宽进行实时监测，当自身接口的流量带宽超过配置的阈值时，新建会话的流量将不再从这个接口转发。当此接口的流量带宽回落到正常值以下时，新建会话的流量再恢复从这个接口转发， |
| 支持基于接口时延的动态切换能力：系统从多出接口向外部某一个或多个目的地址探测时延。当自身接口的时延超过配置的阈值时，新建会话的流量就不再从这个接口转发，而是走其它接口。当此接口的时延回落到正常值以下后，新建会话的流量再允许从这个接口转发 |
| 支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断 |
| 支持IPV6邻居发现协议、IPV6 SNMP管理、IPV6路由配置、IPV6 DNS配置、IPV6策略配置、IPV6 ALG配置、IPV6 6TO4隧道配置、IPV6 4to6隧道配置、NAT-PT配置、NAT64和DNS64配置 |
| ★支持对IPV6用户的会话日志监控、流量监控、应用监控功能，并且能够对IPV6用户进行自定义监控统计功能 |
| 提供SSL VPN功能；必须支持对登录SSL VPN的用户端系统进行端点安全检查，至少包括指定文件、进程、系统补丁、浏览器版本、杀毒软件等方面 |
| **IPS功能** | 支持旁路和在线两种模式，支持基于安全策略和安全域启用IPS功能，可在不同的攻击方向上启用IPS（至少支持流入\流出\双向等方向） |
| 支持CC攻击检测，支持访问限速、代理限速、自定义请求阈值、爬虫友好等方法，检测到CC攻击时支持JS Cookie、重定向、访问确认、验证码四种认证方法 |
| ★具备8000种以上攻击特征库规则列表，并可自定义特征库 |
| **管理功能** | 支持不少于8个配置文件并存，并支持配置文件备注以便配置回退。 |
| 提供手机APP，实施监控展现设备CPU利用率、内存利用率、并发连接数、流量等状态 |
| 通过手机APP提供防火墙威胁分析服务，包括攻击级别展示、攻击类型分析、攻击者和受害者信息统计分析 |
| **资质要求** | ★公安部颁发的《计算机信息系统安全专用产品销售许可证》（防火墙万兆增强级） |
| 具备中国信息安全产品认证中心颁发的《中国国家信息安全产品认证证书》（ISCCC 万兆），提供证明文件 |
| 具备信息产业部颁发的电信设备进网许可证，提供证明文件 |
| 提供近五年入围Gartner企业级防火墙魔力象限证明文件。 |
| **质保授权** | ★投标时提供原厂商针对本项目的授权函和三年售后服务承诺函 |

## 2.态势感知平台(1台)

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 品牌要求 | ★国内外知名品牌，产品必须是自主开发，拥有自主知识产权；能够实现与我院的终端杀毒软件、网络防毒墙、云安全软件等的全面联动分析及响应阻断功能 |
| 性能 | ★支持吞吐量不少于2.5Gbps，最高并发不少于3,000,000 |
| 监听端口 | ★出厂默认不少于6个网口，可扩展2个PCIe插槽，最多可扩展至9个电口，或是4个光口 |
| 扫描对象 | 可扫描网络第2层至第7层数据流量，可选择特定协议或IP地址自定义检测，支持自定义IP地址、URL、域名与文件的访问监控 |
| 支持协议 | 超过 100 种以上的网络协议支持，如 HTTP, FTP, TFTP, SMTP, POP3, IMAP, SNMP, IRC, DNS, DHCP, P2P, SMB, RDP, VNC, TELNET, TCP, UDP和数据库协议（MSSQL, MySQL, Oracle）等。 |
| 移动设备恶意程序侦测 | 可侦测识别iOS、赛班、安卓、微软等移动设备，可与移动应用信誉系统（MRS）联动，侦测安卓系统的恶意应用App |
| 恶意行为分析侦测 | ★威胁流量与协议异常检测 ，如零日攻击、网络蠕虫、木马、后门、僵尸、间谍软件、网络漏洞、网页威胁（网页漏洞、跨网站攻击）、钓鱼邮件、暴力攻击、数据库注入攻击等。 |
| 未知威胁侦测（订制化沙盒分析） | 单台侦测设备具有虚拟化沙盒系统 |
| ★具有安全风险评估技术分析：包含针对注册表、内存、程序、网络活动、文件系统等操作系统环境的变化进行记录与分析 |
| 具有高度定制化，可以支持使用客户环境特性的Windows操作系统平台与应用，服务器级：Windows 2003/2008/2012，用户端级：Windows XP/7/8/10 |
| 提供分析结果的自动入库：侦测设备自我学习功能 |
| 信誉分析 | 支持中国区域恶意网页评估系统，恶意网站与域名分析，僵尸网站与控制服务器分析和移动应用分析 |
| 多协议关联分析 | 能够自动关联不同协议、不同会话的威胁日志，筛选出严重事件，节省事件处理的人力成本 |
| 定制化黑白名单 | 可将企业长期累积的黑白名单（如IP/URL/Domain/File SHA1） 汇入TDA实行侦测或是排除 |
| 常见漏洞检测 | Tomcat写文件漏洞，ImageMagick命令执行漏洞，ElasticSearch 命令执行漏洞，Samba 远程命令执行漏洞, ThinkPHP Builder.php SQL injection, Adobe ColdFusion 文件上传导致任意代码执行漏洞, GhostScript 沙箱绕过漏洞, Spring Data REST PATCH请求代码执行漏洞, Weblogic wls9\_async\_response 反序列化远程命令执行漏洞, Jenkins RCE, Spring Data Commons组件远程代码执行漏洞,spring-messaging Remote Code Execution, Fastjson反序列化漏洞等 |
| WebShell检测 | 支持如下Webshell检测：ghost webshell，PHP webshell2，ASP webshell1，PHP webshell3，PHP Webshell4，ASP webshell\_2 |
| 黑客工具检测 | 支持如下黑客工具攻击检测：Cknife，SQLmap，havij，awvs，Nmap，pangolin，EarthWorm，sql综合利用工具，dirbuster，w3af，OWASP ZAP 2.6.0，Bbscan，OpenVAS，Golismero security scanner, IIS\_shortname\_Scanner, HeartbleedScanner, Heartbleed-msf |
| 威胁流量数据下载 | 支持威胁流量的自动存储，及威胁流量PCAP文件格式下载 |
| 网络流量威胁验伤 | 支持对网络Http攻击流量的应答码及攻击状态展示 |
| 主机威胁联动验伤 | 1. 支持与主机威胁回溯调查的自动验伤功能，支持威胁类型包括如下：  勒索病毒(Ransomwares) ；木马病毒(Trojan)；恶意代码(Malware)；僵尸网络(Botnet)；钓鱼网站(Phishing)；渗透工具；挖矿网址；挖矿病毒；带毒邮件攻击(Mail attack) 2. 支持主机威胁联动验伤报告的自动生成  3. 主机威胁联动验伤报告支持客户自定义徽标功能  4. 主机威胁联动验伤报告支持客户自定义水印功能 |
| 日志管理 | 可显示受感染主机的APT攻击阶段，帮助管理者制定响应策略 |
| 提供智能日志搜寻以及可定制化过滤条件，定制化过滤条件并可支持存储以及汇出汇入，并可快速过滤出常见攻击类别(如勒索软件，横向扩散攻击等) |
| 支持Syslog协议，可以实时传输日志到syslog服务器，选择传输的内容类型,自动检查日志数据库健康与修复数据库, 可以依据时间,协议,威胁类型,IP网段,监控群组等查询条件查询日志 |
| 报表系统 | 自动提供经过分析后的图形化日/周/月报表,自动寄送报表与处理建议功能 |
| ★可集成企业统一威胁预警地图显示，结合地理位置直观标示威胁位置，在地图中实时风险事件定位与威胁流量监控，同时可以区域与威胁事件关连，结合威胁仪表板，深入了解区域威胁情况 |
| 支持多种报表模板 |
| 工具 | 可提供快速响应与专杀工具 |
| 部署 | 支持旁路安装模式,TAP分流安装模式 , |
| 侦测设备自我学习升级 | 沙盒系统分析结果自动回馈到云端大数据平台，更新的pattern可以下发到更多的侦测设备 |
| 联动性 | 能够与威胁阻断系统联动，根据监控结果自动阻止不安全计算机的网络通讯，或是阻断恶意通讯连接 |
| 能与现有内网中杀毒软件通过中央控管中心联动，阻断已知或未知威胁文件 |
| 支持中央管理系统，多台设备可统一管理，多台设备可集中生成报表 |
| 能够集成外接沙盒分析系统，提高未知威胁分析处理能力 |
| Syslog日志为CEF或LEEF格式，可集成第三方SIEM/SOC系统 |
| 提供 Web API 以利第三方集成使用本地威胁情报 |
| 支持调查取证平台 |
| 产品资质 | 产品中所用的引擎必须都是非OEM或引入其他厂商技术，以保证服务支持的连续性，和技术维护的一贯性。所有产品必须是自主开发，拥有自主知识产权，具有软件著作权登记证书 |
| ★具有中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》。 |
| 具有国产软件登记证证书 |
| 服务要求 | 投标商不得随意扩大所投产品的技术功能及性能，以官网公布的资料为准；技术偏离表需逐条应答，签订合同前需提供功能性测试。  ★投标时需提供针对该项目的授权许可函和三年原厂质保函。 |

## 3.数据库审计平台(1台)

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| **数据库安全网关** | 1. 产品结构：1U机架式一体化设备, ≥4个千兆以太网接口，CPU不低于4核，网络吞吐能力≥1000M，SQL语句交易量≥30000条/秒，内存≥8G 2. 部署模式: 支持旁路侦听模式，无需安装Agent，并且能够实现旁路阻断，支持串联透明部署模式，不需要添加任何插件和引擎，支持反向代理部署，支持MACVLAN方式部署； 3. 高可用性：支持三层bypass技术（硬件bypass,软件bypass，程序bypass），支持双机热备； 4. 管控范围：覆盖主流商用数据库，包括：Oracle 8/9/10/11等;Sybase所有版本;SQL Server 2000/2005/2008/2012/2016;Informix所有版本;DB2所有版本;MYSQL所有版本，资产添加简单安全，仅需填写数据库系统IP、端口和版本即可，无需填写数据库账号和密码； 5. ★会话记录：支持以会话为单位的数据库操作过程详细记录，包括但不限于精确的时间点、来源网络地址、来源端口、客户端主机名、数据库实例名、数据库类型、目标地址、目标端口、客户端程序、数据库账号以及完整的操作行为详情； 6. 准入学习：可自动学习数据库操作来源的客户端主机名称、数据库实例名、数据库账号、客户端应用程序等，并在独立页面中进行展示。 7. 网络防火墙：对访问数据库的来源IP及端口的访问进行控制,支持IP或端口白名单策略； 8. 行为防火墙：提供全方位的策略规则匹配，策略因子包括：客户端IP地址、数据库登录用户名、数据库实例名、客户端主机名、客户端应用名、SQL操作语句（DDL、DML、DCL）、数据库表组（表、条件）等告警或阻断匹配条件，支持CIS数据库基线安全模板，至少包含150个规则模板。 9. ★准入防火墙：通过白名单自学习进行访问准入规则的固化，自动学习到数据库访问行为的五元素，通过管理者人为固化安全规则，未被固化的数据库接入行为都会进行实时的告警或阻断，可以识别SQL SERVER 2005/2008/2012/2014/2016数据库访问来源客户端、数据库账号等信息，可对非法访问进行快速有效识别，根据策略可对所有访问来源进行实时的告警或阻断。 10. ★数据库实时监控：监控内容包含但不限定于网络流量、数据包、突发连接数、并发连接数、SQL语句数，并以动态图表实时展示, 提供最近一周内数据库的网络流量、数据包、突发连接数、并发连接数、SQL语句数波形图，并可供下载查看。 11. 统计报表，内置报表需包含且不限于等级保护合规、数据库访问详情、数据库访问统计等类型，每种类型不少于5种。 12. 供货厂商需具备ISO9001质量管理体系认证； 13. 供货厂商需具备中国互联网网络安全威胁治理联盟成员单位证书； 14. 投标产品必须具备计算机软件著作权登记证书 15. ★投标时需提供针对该项目的授权许可函和三年原厂质保函。 |

## 4.边界防毒墙（1台)

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 品牌 | ★国内具备自主病毒引擎知识产权，自主研发，非OEM产品; |
| 支持协议 | 超过100种协议支持, 如 HTTP/HTTPS/FTP/SMTP/POP3/TFTP/TCP/UDP/NFS/SNMP/ICMP/RTMP/DNS/IRC… |
| 应用防火墙 | 二至七层全协议应用防火墙 |
| 用户及终端管理，应用识别及管理，带宽管理及控制，防DoS/DDoS |
| 防恶意软件 | ★防已知恶意软件 (病毒、木马、蠕虫、后门、间谍软件、灰色软件、Rootkits等) |
| 防未知高级恶意程序 |
| APT防护 | C&C违规外联及僵尸网络检测及拦截 |
| 已知文档漏洞检测及拦截 |
| 未知文档漏洞及零日文档漏洞检测及拦截 |
| 可与威胁感知的增强侦测模块联动，获取威胁感知的增强侦测模块侦测到的本地C&C黑名单，并阻止C&C违规外联 |
| 可提交可疑文件、URL、IP及域对象至APT增强定制化沙箱模块DDAn做联动分析，并根据DDAn的分析结果做进一步处理 |
| 入侵检测  及虚拟补丁 | 服务器及终端虚拟补丁和主动式主机入侵防御系统 |
| 防止漏洞利用和SQL注入, 命令注入, Webshell 攻击, XSS 攻击, CSRF 攻击 |
| 主机零日漏洞防护 |
| 8,000+条入侵检测特征库 |
| 配置虚拟补丁功能 |
| Web安全 | URL信誉检测（恶意网站主动实时防御，支持黑白名单，每天十亿网页分析) |
| URL分类过滤（支持自定义URL分类） |
| 钓鱼网站检测 |
| 邮件安全 | 垃圾邮件检测 |
| 恶意邮件检测 |
| 支持邮件黑白名单，支持关键字和正则表达式内容过滤 |
| 支持邮件隔离、带标记转发、记录、清除恶意附件保留邮件正文转发等管理功能 |
| 病毒识别码 | 3,000,000+种病毒识别码，每年约新增750,000+识别码 |
| 全球病毒实验室+本地病毒实验室支持 |
| 本地病毒特征码 (至少百分之二十是中国的特征码) |
| 应用程序侦测 | 全球 1300+ 应用程序协议支持 |
| 点对点 (P2P) 软件控制: Ares,Bittorent,Blubster,eDonkey,Kazaa,Gnutella,Winny,Foxy |
| IM软件登陆及文件控制: AIM,Goggle Talk,MSN,Skype,Yahoo messenger |
| 网络游戏控制，文件服务器软件控制，精简客户端软件控制，Web应用控制，Web邮件控制 |
| 无界,自由门软件控制 |
| 带宽控制 | 支持基于策略（源和用户/目标/通讯类型/时段）的带宽控制 |
| 支持上行流量/下行流量的带宽控制 |
| 日志管理 | ★提供安全日志/流量日志/VPN日志/系统日志/审计日志的查询/打印/导出 |
| 提供基于策略（源和用户/目标/通讯类型/时段）的流量日志记录/查询/打印/导出，可按照时间，协议，威胁类型等查询条件查询日志 |
| 支持Syslog协议，可以实时传输日志到Syslog 服务器 |
| 可靠性 | 系统保证36 月, 下一个工作日提供备机 |
| 提供Fail Open功能，在停电与系统出现问题时自动实现直通功能 |
| ★配置性能要求 | 高级应用防火墙吞吐量≥10Gbps；  高级应用防火墙 ＋ 防病毒≥4Gbps；  高级应用防火墙 ＋ IPS + 虚拟补丁≥5Gbps  SSL用户数≥无限制  安全功能同时全开吞吐量 (高级应用防火墙 + IPS + 虚拟补丁 + APT防护 + 防病毒 + Web信誉 + 邮件信誉) ≥3Gbps  最大并发会话数≥160万  每秒新建会话数≥5万  管理接口≥1×配置口 ，2×USB 2.0口  网络接口≥8×千兆电口（支持3组bypass）  可扩展接口≥4×千兆电口 或4×千兆光口或2×万兆光口  电源≥ 250W电源 |
| 厂商 | 厂商可根据用户需求提供高级别的服务承诺，如大客户专署服务、主动式服务、快速响应服务(SLO/SLA)、在线技术支持服务等，可提供7×24小时的专业防毒服务 |
| 通过CMMI5认证 |
| 具备国家计算机病毒应急处理中心技术支持单位 |
| 产品 | 产品中所用的防病毒引擎，病毒代码，防病毒扫描原理, APT侦测, 入侵检测, 虚拟补丁,Web信誉, 防垃圾邮件等都必需为厂商自有技术，以保证服务支持的连续性，和技术维护的一贯性。 |
| ★产品具备公安部“防病毒网关”销售许可证 |
| 其他要求 | 投标商不得随意扩大所投产品的技术功能及性能，以官网公布的资料为准；技术偏离表需逐条应答，签订合同前需提供功能性测试。  ★投标时需提供针对该项目的授权许可函和三年原厂质保函 |

## 5.集成服务

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| ★基本要求 | 1. 提供本次所有软硬件产品的安装与调试服务； 2. 提供虚拟化平台业务梳理服务； 3. 提供每月至少一次巡检，并提供巡检报告； 4. 提供三年系统集成服务。 |