# 附件：[安吉县卫计局安全设备技术参数](file:///E%3A%5C%5C%E8%BF%AA%E8%B4%B8%E7%A7%91%E6%8A%80%5C%5C2018%5C%5C%E5%AE%89%E5%90%89%E5%8E%BF%E5%9B%BD%E5%9C%9F%E8%B5%84%E6%BA%90%E5%B1%80%5C%5C%E5%AE%89%E5%90%89%E5%9B%BD%E5%9C%9F%E6%9C%AC%E5%9C%B0%E5%AD%98%E5%82%A8%E5%8F%8C%E6%B4%BB%E5%8F%8A%E4%B8%8D%E5%8A%A8%E4%BA%A7%E7%99%BB%E8%AE%B0%E5%AE%89%E5%85%A8%E7%B3%BB%E7%BB%9F%E5%BB%BA%E8%AE%BE%E9%A1%B9%E7%9B%AE%E8%A7%84%E5%88%92%E6%96%B9%E6%A1%88%5C%5C%E9%A1%B9%E7%9B%AE1%5C%5C%E8%AF%A2%E4%BB%B7%E4%BF%A1%E6%81%AF1%EF%BC%9A20181011%E5%AE%89%E5%90%89%E5%9B%BD%E5%9C%9F%E5%AD%98%E5%82%A8%E5%8F%8C%E6%B4%BB%E5%BB%BA%E8%AE%BE%E9%A1%B9%E7%9B%AE.docx%22%20%5Cl%20%22_%E6%A1%90%E4%B9%A1%E5%9B%BD%E5%9C%9F%E8%AE%BE%E5%A4%87%E6%89%A9%E5%AE%B9%E8%AF%A2%E4%BB%B7%E5%8D%95)配置要求表及商务要求

|  |
| --- |
| 防火墙-招标参数 |
| **技术指标** | **技术配置要求** |
| ▲兼容性 | 可实现与原有防火墙（深信服）双机热备功能 |
| ▲性能配置 | 产品为标准2U机架式设备，需满足多核X86架构。标配10个千兆电口，4个千兆光口。并含2个高速USB2.0接口，1个RJ45串口，性能配置需满足：整机吞吐量≥10Gb；应用层吞吐量≥2Gb；并发连接数≥2200,000；每秒新建连接数≥120,000；硬盘≥ 1TSATA盘，冗余电源，支持BYPASS。 |
| 基础功能 | 支持根据国家/地区来进行地域访问控制；（需提供截图证明） |
| 能够识别应用类型超过1200种，应用识别规则总数超过3000条； |
| 支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制； |
| 支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式；支持在防火墙上配置VPN安全策略对加密隧道内的流量进行清洗； |
| 支持配置向导功能，并提供攻击源IP的攻击地图展示；攻击地图需包括攻击时间，攻击源归属地和IP，被攻击者IP，攻击类型和危害等级及当日安全事件统计（需提供截图证明） |
| DoS攻击防护 | 支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护、支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测； |
| 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； |
| 内容安全 | 内置病毒样本数量超过200万；支持URL过滤和文件过滤功能，URL过滤支持GET，POST请求过滤和HTTPS网站过滤，文件过滤支持文件上传和下载过滤；▲支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤；（需提供截图证明）  |
| 入侵防护 | 为了保证入侵防御系统识别的专业性，要求入侵防护漏洞规则特征库数量在7000条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号，参考信息和建议的解决方案；（需提供截图证明） |
| 为了避免因黑客暴力破解导致的密码泄露事件，要求设备支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；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； |
| 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间； |
| 为了帮助管理员更好的应对一些突发的热点安全事件，要求设备可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；（需提供截图证明） |
| 僵尸主机检测 | 设备具备独立的僵尸网络识别库，特征总数在40万条以上； ▲支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；（需提供截图证明）对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告；（需提供相关证明）支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；（需提供相关云端大数据分析能力的证明）  |
| 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；▲支持对检测到的攻击行为按照IP地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息；（需提供截图证明） |
| 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；  |
| ▲支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况；（需提供截图证明） |
| 安全管理中心 | 为了更好的管理多台设备，要求支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能。 |
| 提供管理员登录失败，SSD磁盘寿命风险，路由异常，邮件安全，IPS，web应用防护，DOS/DDOS攻击及僵尸网络邮件告警 |
| 安全监控平台可以查看到每台安全设备最近的有效安全事件及安全有效事件趋势图，支持根据每台安全设备的最近的安全趋势进行安全状况分级； |
| ▲支持安全策略一体化配置，通过一条策略既可实现不同安全功能的配置；（需提供截图证明） |
| 自动运维 | 针对黑链检测 Webshell、检测高级黑客攻击、密集型攻击、持续型攻击、僵尸网络、外发DOS攻击6类安全事件，提供微信告警（提供截图证明） |
| ▲针对防火墙策略实时给出优化建议使设备处于最佳状态（需提供截图证明） |
| 针对设备硬件状态、设备软件、状态版本信息、策略信息、网络基础状态线上巡检 |
| ▲产品资质 | 厂商具备CMMI L5认证证书（需提供证明材料） |
| 产品应具备ISCCC中国国家信息安全产品认证证书；（需提供证明材料） |
| 具备IPv6 READY认证证书（需提供证明材料） |
| 产品成熟度 | 要求所投产品Web应用防护能力经过国际知名实验室NSS Labs测试，并获得recommended推荐级别；（提供NSS Labs相关测试报告并加盖厂商公章） |
| ▲产品测试 | 中标后二个工作日内需要提供所投品牌型号的样机进行上述功能要求的逐一测试验证，全部通过后执行合同流程，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为将予以废标处理并保留对预中标单位和厂商追究相关责任的权利 |
| ▲售后服务 | 提供设备初次原厂工程师现场安装服务；质保期内提供3年7\*24免费软硬件（免上门费、备件费、人工费等相关费用）原厂技术支持与上门售后服务；中标后二个工作日内提供原厂商三年质保和7x24小时售后服务承诺函 |
| 日志审计系统-招标参数 |
| **技术指标** | **技术配置要求** |
| ▲品牌 | 为了保证系统稳定性和提高维护效率，要求与防火墙同一品牌 |
| ▲系统架构 | 产品结构 | 要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁； |
| 系统许可方式 | 内置50个主机审计许可证书； |
| 产品架构 | 采用标准2U机架式硬件 |
| 操作系统 | 深度定制优化的Linux系统； |
| 管理方式 | B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端； |
| 设备部署 | 提供旁路接入模式，设备部署不影响原有网络结构； |
| 数据存储 | 所供系统设备必须自带本地存储功能；可用物理磁盘空间>=1TB；日志存储量至少十亿条；（指标以原厂公开资料为准）；RAID架构以保证数据可靠性,（指标以原厂公开资料为准）；支持后期扩展外部网络存储(IP SAN、NAS、DAS、磁盘阵列等)； |
| 网络接口 | 审计主机至少提供千兆RJ45\*6（一路数据传输口；一路系统管理口）；网络接口支持电口，可升级为光口； |
| 处理性能 | 日志采集能力：3000条/秒以上 |
| 功能要求 | 数据采集 | 支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、Glftpd、Serv-u]；支持SNMP日志采集，支持日志类型：网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]▲支持Opsec Lea日志采集；（提供产品页面截图证明）支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览、论坛微博]、入侵检测、业务检测、流量监控；▲支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储；（需提供截图证明）支持文本型日志原始文件管理，可将系统作为日志服务器使用；（需提供截图证明） |
| 基本功能 | 监控功能 | 支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况；支持自定义配置实时监控的日志类型；支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警；支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况；支持实时监控系统当前运行状态，包括系统CPU、内存、硬盘状态及管理员操作； |
| 报表分析功能 | 系统内置多种类报表模板；支持动态\静态（日报、周报、月报）两种系统生成方式；支持报告的邮件转发、生成提醒功能；支持多人邮件接收；支持自定义审计报告；支持导出html、Excel、PDF；支持管理员自定义审计报表模板；（需提供截图证明） |
| 查询分析功能 | 支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索；（需提供截图证明）支持以日志类型、时间范围及条件字段快速检索过滤；支持高级检索以多条件组合查询方式，可以将每一个日志字段作为查询条件进行查询；支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件；支持查询模版创建、修改、删除功能；（需提供截图证明）支持查询结果导出； |
| 策略管理功能 | ▲支持内置归并策略，对HTTP数据进行自动归并处理；（需提供截图证明）支持内置关联分析策略，可设定用户在规定时间内连续多次输入错误口令产生告警或事件；支持数据策略，可设定采集多种WEB访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问；（提供产品页面截图证明）支持自定义创建实时审计规则：根据日志字段为条件预设置分析策略； 规则条件设定支持逻辑运算符与支持正则表达式；（需提供截图证明）支持自定义三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息；（需提供截图证明）支持以告警页面、短信、邮件、SYSLOG、SNMP等各种方式呈现告警信息； |
| 数据管理功能 | 支持按日志属性、日志类型、时间范围进行数据备份；（需提供截图证明）支持WEB界面备份及日志恢复导入工作；支持自动与手动两种备份归档方式；▲系统支持以FTP上传方式将归档文件存储到第三方存储系统中；（需提供截图证明） |
| 系统配置功能 | 支持审计系统用户（组）管理（添加、修改、删除、停用、启用）；支持资产管理，即所有采集日志源管理维护；支持密码长度、复杂度，密码猜测自动锁定账号以及系统超时设置安全策略；支持证书页面生成下载；支持系统配置备份恢复；支持时间同步页面配置；支持页面方式系统升级以及设备关闭、重启；支持从WEB界面查看网卡IP设置，修改静态路由设置等内容；支持安全页面（SSL）证书下载；（需提供截图证明） |
| 系统安全 | 系统自身安全 | 系统内置安全防火墙；支持控制访问审计主机范围；必需提供内部通讯检查机制，传输128加密；管理接口支持串口或电口的方式管理；管理界面与其他功能模块分离； |
| 日志数据安全 | 审计日志文件方式存储；审计日志加密导出审计系统；支持对所有审计管理员操作审计系统的动作进行审计； |
| 日志权限 | 审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明；（提供产品页面截图证明）支持日志类型、IP地址权限设置；支持页面功能模块权限设置； |
| 系统升级二次开发 | 在设备维保期内，厂家提供对系统软件的免费升级服务，保证系统软件为最新版本；根据用户需求定制开发相关内容，包括关联报表和特定业务日志审计等功能； |
| ▲资质要求 | 产品资质 | 公安部《计算机信息系统安全专用产品销售许可证》；国家版权局《计算机软件著作权登记证书》 |
| 厂商资质要求 | 厂商具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（二级）厂商具有中国信息安全测评中心颁发的信息安全服务资质（安全工程类一级）厂商具有国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书（国家级）厂商具有中国信息安全认证中心颁发的信息安全服务资质，风险评估（二级）厂商具有中国信息安全认证中心颁发的信息安全服务资质，应急处理（二级）厂商具有国家信息中心与网络安全部颁发的国信安全服务支撑单位证书 |
| ▲产品测试 | 中标后二个工作日内需要提供同型号的样机进行上述功能要求的逐一测试验证，全部通过后执行合同流程，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为将予以废标处理并保留对预中标单位和厂商追究相关责任的权利 |
| ▲售后服务 | 提供设备初次原厂工程师现场安装服务；质保期内提供3年7\*24免费软硬件（免上门费、备件费、人工费等相关费用）原厂技术支持与上门售后服务；中标后二个工作日内提供原厂商三年质保和7x24小时售后服务承诺函 |
| 数据库审计系统-招标参数 |
| **技术指标** | **技术配置要求** |
| ▲品牌 | 为了保证系统稳定性和提高维护效率，要求与防火墙同一品牌 |
| ▲性能要求 | 性能指标：单向数据库流量800M 硬件指标：2U，单电源，6个千兆电口+4个千兆光口，2TB SATA硬盘 |
| 部署方式 | 审计方式：旁路交换机镜像 、 Agent抓包 |
| 数据库审计旁路镜像模式部署不影响数据库性能和网络架构；  |
| 部署方式：单机（采集器）、多机（管理器） |
| 多机部署支持集中管理，可集中管理多台采集器审计的事件、分析，实现统一配置、统一报表、统一查询； |
| 部署环境： 支持虚拟化平台部署 |
| 支持导入到主流虚拟化平台以模板的方式部署 |
| ▲支持多种虚拟化平台，包括Sangfor-HCI (vma格式)、Kvm (qcow2格式)、Vmware (ova格式) |
| 部署管理 | 采用B/S管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务。 |
| 支持IPv6协议可识别IPv6协议的数据流，支持基于IPv6地址格式的审计策略。 |
| 审计能力 | 支持多种数据库类型的审计，支持Oracle数据库审计、SQL-Server数据库审计、DB2数据库审计、MySQL数据库审计、Informix数据库审计、达梦数据库审计、人大金仓数据库审计、postgresql数据库审计、sysbase数据库审计、cache数据库。 |
| 支持同时审计多种数据库及跨多种数据库平台操作 |
| 支持在windows平台上安装插件的方式审计，插件方式更快捷更稳定，无需改变系统内核和驱动的原有工作方式来支撑审计，有效防止修改内核或驱动带来的系统崩溃隐患。 |
| 超长SQL语句解析、记录、账号、关联SQL操作语句绑定变量参数。 |
| ▲支持白名单审计：系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌，白名单内容包括以下4个维度 |
| 1 SQL模版：支持通过SQL模板作为数据库条件来过滤，SQL模板来源方式包括已有的SQL模板、自动生成的SQL模板 |
| 2 业务系统：支持通过自定义设定业务系统作为白名单条件，包括全部业务系统、自定义单个或多个业务系统 |
| 3 URL地址：源IP、业务系统、生效时间、URL地址 |
| 4 数据库条件：源IP、业务系统、生效时间、客户端程序、数据库用户、数据库名、表名、操作类型 |
| 支持客户端程序、数据库用户、操作类型、数据库名表名、响应时间、返回行数、影响行数、响应内容等实现对敏感数据库操作的精细审计；  |
| 支持HTTP请求审计，包括GET、POST、URL、响应码进行精细审计。 |
| 支持时间段、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索。 |
| 支持时间段、源IP、业务系统、搜索关键字等对WEB审计日志进行精细检索。 |
| 支持日志导出到execl |
| 深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源IP、源端口、源MAC、目的IP、目的端口、数据库用户、数据库类型、操作类型、SQL语句、SQL模版、客户端程序名、响应码、影响行数、返回行数、SQL预计响应时间。 |
| 支持三层架构下web要素审计。 |
| 独立不漏审机制保障独有的应用层接管内核技术保障永不宕机，专用CPU机制保障收发数据不丢包； |
| 允许查看SQL语句会话日志、柱状图、会话视图等。 |
| 审计SQL模版：产品支持自动基线学习数据库语义语法，并支持提取参数自动生成SQL模板，可以减少审计日志的重复写入和节省磁盘的存储空间 |
| 安全能力 | ▲内置大量细粒度SQL安全规则包括如下：内置大量的SQL安全规则可以针对导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp\_addrolemember 提权、web端sp\_addrolemember提权、查询内置敏感表、篡改内置敏感表等。 |
| 支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断。 |
| SQL语句安全检测：爆库、撞库 |
| 识别当前的SQL操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施。 |
| ▲支持基于SQL命令的webshell检测提供webshell日志查询可通过查看webshell攻击的时间、源IP、业务系统、webshell规则发现威胁 |
| ▲支持联动其他安全设备（如下一代防火墙）实现webshell阻断，提供webshell日志查询，可通过查看webshell攻击的时间、源IP、业务系统、webshell规则发现外部威胁，提供界面截图，并加盖生产厂商公章。 |
| 统计分析 | 支持以源IP、业务主机、操作类型、SQL模版、数据库用户为维度的数据库行为排行。 |
| 支持以源IP、业务主机、操作类型、SQL模版、数据库用户为维度的数据库行为趋势。 |
| 支持以新型SQL趋势统计、支持SQL响应性能分析。 |
| 支持执行SQL语句失败分析，包括登录失败排行，SQL语句失败排行。 |
| 支持吞吐量分析，包括SQL语句吞吐量排行、SQL语句吞吐量趋势、SQL操作类型吞吐量排行、SQL操作类型吞吐量趋势、数据库用户吞吐量排行、数据库用户吞吐量趋势、业务主机吞吐量排行、业务主机吞吐量趋势。 |
| 精细化审计日志分离存储通过SQL串模式抽取保障磁盘IO的读写性能；分离式存储SQL语句保障数据审计速度快 |
| ▲TB级日志秒级查询支持指定源IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多SQL语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询。 |
| 支持报表收藏，报表导出PDF。支持报表订阅，自定义报表。 |
| 风险分析 | 支持以时间、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL模版为条件的数据库风险查询。 |
| 支持以风险级别、源IP、业务主机、数据库用户、风险类型为维度的数据库风险排行。 |
| 支持以风险级别、源IP、业务主机、数据库用户、风险类型为维度的数据库风险趋势。 |
| 支持Syslog告警、SNMP trap告警、邮件告警，短信告警，包括支持SNMP TRAP方式，提供系统运行状态给第三方网管系统； |
| 旁路主动发rest包阻断技术Netfilter框架技术可灵活针对IP、端口、业务系统做精准阻断。 |
| 响应方式 | 提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。 |
| 管理员支持下面几种角色 |
| （1）. 超级管理员（仅admin，不能新增，仅一个） |
| （2）. 安全管理员（负责配置规则, 无查看日志权限) |
| （3）. 审计管理员（负责审计日志，仅有日志查看权限） |
| （4）. 自定义角色：可以自选页面 |
| 支持系统异常、磁盘空间占用过高、采集器离线等告警。 |
| 系统管理 | 支持日志备份和日志恢复。 |
| 支持系统日志查看，系统升级，重启操作，磁盘空间自动删除系统必备功能。 |
| 可以实时监控系统的CPU使用率，内存使用率和磁盘占用率。快速定位系统的负载压力和系统运行状况。 |
| 支持Syslog方式向外发送审计日志； |
| 数据灾备 | 数据可靠性及灾备（1）. 独有的Mapreduce框架支持自动将数据同步到外部备份（2）. 支持数据到磁盘柜、RAID阵列卡（3）. 支持针对原始数据实现事物重做，来保障数据的灾备 |
| ▲资质证明 | 设备生产厂商注册资本不小于6000万； |
| 中国信息安全认证中心(ISCCC)证书-增强级； |
| 公司研发体系通过国际认证CMMI5； |
| 售后服务体系通过ISO9001认证； |
| 国家应急中心应急支撑单位CNCERT证书； |
| 产品获得公安部数据库审计产品《计算机信息系统安全专用产品销售许可证》； |
| ▲产品测试 | 中标后二个工作日内需要提供同型号的样机进行上述功能要求的逐一测试验证，全部通过后执行合同流程，在指定的时间不能提供测试样机进行测试或测试中发现虚假应标的行为将予以废标处理并保留对预中标单位和厂商追究相关责任的权利 |
| ▲售后服务 | 提供设备初次原厂工程师现场安装服务；质保期内提供3年7\*24免费软硬件（免上门费、备件费、人工费等相关费用）原厂技术支持与上门售后服务；中标后二个工作日内提供原厂商三年质保和7x24小时售后服务承诺函 |

**商务要求**

1. 仅限安吉地区供应商

2、〈一〉中标人应免费将所供产品运输到用户指定地点，用户组织产品供货验收合格后，根据用户要求免费实施产品的安装调试。 〈二〉根据用户实际应用的要求，免费提供产品的安装调试，应包含项目所需相应的所有附件等材料。 ▲〈三〉质保期三年，中标后二个工作日内需提供原厂商针对本项目的三年7x24小时售后服务承诺函原件、原厂商盖章的技术参数响应表（如多页，每页需盖章）、询价单要求的证明材料并加盖公章及产品到用户现场进行测试，如达不到要求的，则按提供虚假材料处理，并取消其中标资格。

3、付款方式：所有设备到货用户核对后并安装调试完毕验收合格支付95%，剩余5%质保金6个月后如无质量问题一次性支付完毕。

4、〈一〉安装地点：安吉县卫计局指定安装地点。 ▲〈二〉完成时间: 2018年12月15日前，必须将所有设备调试安装完毕。〈三〉安装标准：符合我国国家有关技术规范要求和技术标准，所有的设备必须保证同时安装到位。 〈四〉中标人免费提供中标设备的安装服务。 〈五〉调试所需专用工具设施材料由中标方自备、自运到现场，完工后自费搬走。

5、〈一〉质保期内因不能排除的故障而影响工作的情况每发生一次，其质保期相应延长60天，保质期内因设备本身缺陷造成各种故障应由卖方免费技术服务和维修。〈二〉在质保期内，所有因服务、设备及零部件更换和维修等原因产生的费用由供应商承担。同时,在整个产品使用期内中标人应确保产品的正常使用，在接到用户维修要求后应立即作出回应，当系统的软硬件设备出现故障时，供应商也应承诺在接到买方通知后30分钟内响应并提出解决方案，在1小时以内完成甲方提出的维修要求，如需更换设备或送修，必须在1个工作日内负责解决。如无法解决问题，应提供同档次的设备予以代用。

7、本次所提供的设备最终用户为：安吉县卫计局