**1.项目名称：铜仁市妇幼保健计划生育服务中心网络安全等级保护项目采购及安装**

**2.项目编号：TRZFCG-2020-018**

**3.公示期限（不少于2个工作日）:**

**2020年4月24日-2020年4月26日**

**4.采购预算：1420000.00元（最低限价1420000.00元）**

**5.采购预算确定依据:**

**铜仁市直政府采购（集中采购）申请表**

1. **采购人名称: 铜仁市妇幼保健计划生育服务中心**

**联系地址: 铜仁市妇幼保健计划生育服务中心**

**项目联系人:王科长**

**联系电话:18608568973**

**7.采购代理机构全称:铜仁市公共资源交易中心**

**联系地址:铜仁市公共服务中心四楼（川硐麒龙国际会展城）**

**项目联系人:张琰**

**联系电话:0856-3912922**

**8.任何单位和个人对本项目采购文件需求公示有异议的，可在公示期限内，反馈意见给代理机构。**

**用户需求见附件**

采购需求

采购人保留测试权限，如采购人对中标人所投产品功能存在疑惑，中标方需在公布中标结果后3个工作日内到采购方进行参数测试，测试通过后由采购方出具测试通过函,再给予发放中标通知书。如果测试发现中标人有虚假应答情况则取消其中标人资格，并由第二中标人候选人继续测试，测试通过后由最终用户出具测试通过函,再给予发放中标通知书。以此类推。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **数量** | **参数需求** |
| 1 | 下一代防火墙 | 3台 | 1、主机配置≥6个10/100/1000M Base-TX；≥2个SFP光口插槽；吞吐量≥2.2Gbps，系统具备防火墙访问控制、流量控制、病毒防护、入侵防护、web防护、应用识别功能； ★2、具备系统主要防护功能的统一化模版设置，模版分为高、中、低三个级别，分别对应不同防护强度，可通过Web界面单击选择切换；按功能模块的配置导入导出功能（提供截图证明并加盖原厂商鲜章） 3、具备基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路）、必须具备基于 WEB地址URL的策略路由，可实现将不同类型的网站流量智能分配到不同的链路）、必须具备基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。 4、具备ISP路由，具备联通、电信、教育网、移动等ISP服务商地址列表，列表可导出及导入，可通过Web界面选择不同的ISP服务商实现快速切换。 ★5、具备一体化安全策略配置，可以通过一条策略实现用户认证、IPS、防病毒、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能,简化用户管理。 ★6、具备将源MAC作为独立的访问控制条件，防止非法设备接入、具备同一个地址对象中可以包含IP、IP段、IP range、排除地址等多种类型。 7、具备针对策略中的源、目的地址进行并发限制，可以针对单IP(或地址范围)进行并发控制、具备针对策略中的源、目的地址进行新建限制，可以针对单IP(或地址范围)进行新建控制。 具备基于策略的入侵检测与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的入侵防护策略。 ★8、SSL VPN具备≥20个并发用户授权，不需要单独付费. 9、支持IPv6安全控制策略设置，能针对IPV6的目的/源地址、目的/源服务端口、服务、扩展头属性等条件进行安全访问规则的设置； 10、支持基于IP、协议、连接数的方式统计会话，统计结果可导出，提供统计会话界面截图证明（提供截图证明并加盖原厂商鲜章）； ★11、支持基于IP层以上的各种TCP/IP协议的应用。包括：http，Email，Ftp，网上邻居，Notes，Outlook，Oracle, SQL等各种动态和静态的C/S应用；支持内网DNS、支持对应用的透明访问、自动定位URL、支持隐藏服务、应用的快捷方式、自动启动服务。（提供截图证明并加盖原厂商鲜章） 12、提供三年硬件质保、三年病毒库升级、三年入侵防御特征库升级及三年质保；  13、提供公安部销售许可证。   1. 计算机软件著作权登记证书；   ★15、提供EAL3+测评证书；   1. 提供中国国家信息安全产品认证证书；   ★17、提供原厂商针对本项目授权书与售后服务承诺函；  ★18、为证明厂商的安全服务能力，需要提供如下资质：中国信息安全认证中心信息安全应急处理服务资质（一级）、中国信息安全认证中心信息安全风险评估服务资质（一级）、中国信息安全认证中心信息系统安全集成服务资质（一级）、国家信息安全测评信息安全服务资质(安全工程类二级）； |
| 2 | 日志审计系统 | 1台 | 1、 日志分析具有日志收集、存储、查询、关联分析、统计分析、上下级管理、自定义告警等功能。 日志处理均值20000EPS，峰值可以达到35000EPS。  2、 支持代理分布式部署采集日志。  3、 日志存储不低于10000条/M，具有数据压缩加密存储能力，压缩比不低于10:1； 支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于10s。  4、 支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于20类300种日志对象的日志数据采集。  5、 支持对每个日志源设置过滤条件规则，自动过滤无用日志。  6、 支持根据设备重要程度设置独立设置每个被采集源的数据存储时间为1月、3月、6月和永久保存等参数。  7、 支持日志备份功能，支持本地备份和FTP备份方式，支持自动备份和手动备份。  8、 设备具有公安部颁发的销售许可证 |
| 3 | 运维审计系统 | 1台 | 1、标准1U硬件，电管理口≥2个，千兆电业务口≥4个,硬盘≥1T；1个RJ45串口，资产数授权≥100个，最大字符并发连接≥100个，最大图型并发连接≥20个。 ★2、 支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据。（需提供相关截图证明并加盖原厂公章） 3、身份认证：支持双因子认证模式，认证方式大于3种，支持基于不同的用户设置不同的双因子认证模式。 ★4、支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权 （需提供国家权威机构证明并加盖原厂公章） 5、设备信息安全：设备信息文件支持加密导出，导出的设备信息文件加密存储，解密时须由2个管理员同时解密才能查看到设备信息文件内容 ★6、支持DB2、oracle、mysql、sqlserver主流数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机（须提供相关截图证明并加盖原厂公章） ★7、支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备；（须提供相关截图证明并加盖原厂公章） ★8、 支持在mac电脑里使用navicat工具通过堡垒机登录mysql、oracle等数据库服务器（须提供相关截图证明并加盖原厂公章） 9、安全联动：支持和同品牌数据库审计系统进行联动，将通过SSH/RDP等加密方式操作数据库的行为整合到数据库审计中，实现数据库行为的统一集中查询、展示、审计分析等； 10、提供销售许可证、IPV6认证证书、CNNVD兼容性认证证书  ★11、提供原厂商针对本项目授权书与售后服务承诺函； |
| 4 | 数据库审计（含防统方模块）系统 | 1台 | 1.标准2U硬件，网口类别千兆电口≥6个；硬盘≥2T，内存≥16G，单电源，吞吐能力≥1000M，双向审计流量≥120mbps；峰值事务处理能能力：12000（条/秒），日志数量存储：10亿条，含软件基本模块； 2.部署方式：支持传统流量镜像方式部署；支持级联分布式部署；支持虚拟化环境部署； 3.协议支持：支持oracle、mysql、db2、sybase、infomix、mssqlserver、https、HTTP、TelnetFTP、SMTP、POP3、DCOM、SQLserverTDE。 ★4.支持自动式一键排错流程，无需管理员具备非常专业的技能即可非常方便的处理设备故障情况，提升故障处理能力（提供截图证明并加盖厂商公章）。 5.内置攻击特征库，特征库数量大于300条。 6.支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小。 ★7.支持对SQLserver（2005及以上版本）数据库采用加密协议通讯，可以通过导入证书的方式实现审计和防护；（需提供功能截图，并提供国家权威检测机构检测报告）。 8.报表管理：内置不少于15种维度的报表，支持自定义报表。 9.支持扫描数据库漏洞和不安全配置。 ★10.支持对数据库自动建模及智能对异常行为告警功能；（提供产品功能截图，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告证明）。 11.可基于账号、IP地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警。 ★12．可通过行为轨迹图方式展示数据库访问行为；（提供截图证明并加盖厂商公章）； ★13. 支持B/S业务系统三层关联审计； （需提供功能截图，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告）。 14.产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》，级别EAL3+，提供证书复印件。产品具备IPV6认证证书； 15产品通过国家信息安全认证中心3C认证检测，级别增强级以上，提供证书复印件；  ★16、提供原厂商针对本项目授权书与售后服务承诺函； |
| 5 | 网闸 | 1台 | 标准化机架设备， 内端机6个千兆接口，2个SFP插槽，1个扩展槽位； 外端机6个千兆接口，2个SFP插槽，1个扩展槽位； 配置应包含文件传输模块、邮件访问模块、VOIP访问模块、数据库访问模块、自定义访问模块、数据中心模块。内外端机双侧液晶屏；  网络吞吐量≥600Mbps；并发连接数≥12万；内外端机各1TB硬盘。  2、系统架构“2+1”系统结构，内外端机为TCP/IP网络协议的终点，阻断TCP/IP协议的直接贯通。内外端机之间采用专用硬件和专用协议进行连接，不可编程。网闸以软硬件结合的方式，有效地隔断内外网络间直接的连接，防止信息无限制交换。  3、采用自研安全操作系统、能够对两个主机系统提供多层次、高强度的安全防护，保护其重要进程、文件、数据不受黑客侵袭。  4、设备支持有客户端和无客户端两种文件同步方式。无客户端方式无需在用户服务器上安装任何插件，网闸不开放任何服务端口；  5、支持对多种主流数据库,如：MYSQL、SQLSERVER、ORACLE、DB2、SYBASE等系统的安全访问。支持多种主流数据库系统之间同步。  6、支持达梦、人大金仓等国产数据同步。 支持客户端与网闸数据摆渡通道数据特征绑定，确保只有授权的合法数据表记录可以通过网闸。  7、支持日志审计功能，包括系统日志、管理日志、访问日志、攻击防护日志、内容过滤日志。  8、设备具有公安部颁发的销售许可证。 |
| 6 | 综合漏 扫 | 1套 | 包含三年之内每年至少两次对主机机操作系统漏扫、应用漏扫、网络及安全设备安全配置检查等功能实现对网络资产的脆弱性评估。 |
| 7 | 数据库双活容灾系统 | 1套 | 1、提供直观的简体中文图形化WEB操作控制台，可以在一个WEB图形界面里管理所有业务系统的容灾系统管理, 要求所有容灾功能统一在WEB界面上操作，应用于HIS系统1个容灾授权。  2、操作系统支持：AIX，HP-UX，Linux，Windows，Solaris等。  ★3、实现所有数据库内的数据操作的复制，包括INSERT\UPDATE\DELETE、DDL操作、Create table ..as 语句，ROWID相关语句等。（需提供相关证明材料）  4、支持虚拟化环境内的各类文件及数据的同步。  ★5、实现所有数据库内的所有对象复制，包括普通表格、压缩表格、临时表格、垃圾箱内的闪回表格等。（需提供相关证明材料）  ★6、要求两个库之间的所有对象完全相同，包括ROWID，基表，视图，同义词，自定义TYPE，IOT表格，SYS用户内的所有对象等。（需提供相关证明材料）  ★7、要求支持误操作闪回服务，支持使灾难备份回到过去的某一时刻点，实现误操作等逻辑错误的灾难恢复。（需提供相关证明材料）  ★8、要求采用物理同步方式，无需考虑复杂的内部数据关系，支持数据库中所有对象的同步，支持所有DDL、DML等语句的复制。（需提供相关证明材料）  9、RPO要求：要求实现数据零丢失，支持同步和异步模式。  10、RTO要求：要求容灾切换在5分钟内完成。  ★11、实现短时间内（比如30分钟的硬件升级）的计划性维护切换以支持日常运行涉及时间比较长的运行维护操作，实现从生产系统切换至容灾系统，从容灾系统切换回生产系统系统。支持一键式切换管理。（需提供相关证明材料）  ★12、要求提供容灾系统桌面演练服务，能够在“沙盘”环境中模拟整个容灾切换过程，桌面演练可以在生产系统业务高峰期间进行，不增加生产系统额外资源开销（包括CPU\内存\IO），不影响业务的继续运行。（需提供相关证明材料）  ★13、提供可视化、直观化、前台界面可操作的WEB管理过程，支持一键切换（一键启动、一键关闭），不需要复杂的流程即可完成容灾切换。（需提供相关证明材料）  14、能够避免逻辑错误传播，从而对于逻辑失败形成根本性的保护。  15、能够防御自然灾害（地震，火灾，雷击等）引起的站点失败恢复。防御大面积电力故障等非自然灾害引起的站点失败恢复。防御主机，存储以及其他IT物理部件失败或者电力故障引起的物理部件失败灾难恢复。  ★16、提供原厂商针对本项目授权书与售后服务承诺函； |
| 8 | 数据库迁移 | 1次 | HIS系统数据库迁移至相对更安全的linux平台。保障HIS系统数据库在linux平台下仍能正常运行HIS系统。 |
| 9 | 威胁分析预警平台 | 1套 | "1.硬件规格：一体化2U标准机架式设备；电源：双电源；内存≥8G； 硬盘容量≥1T，接口数量：千兆电口≥6个；吞吐率：网络层≥1Gbps；应用层≥500Mbps；  2.支持WEB检测：HTTP最大并发数≥7万/秒；支持邮件检测：邮件处理数≥100万封/24小时；文件检测≥3万个/24小时  3.部署方式：支持旁路部署和分布式部署，对探测器可以添加、删除，显示探测器版本、状态和IP，管理中心可实现告警统一管理；可自定义管理中心和探测器之间的数据传输速率、时间、发送目录等参数；  4.支持全流量检测，可根据需求打开或关闭全流量检测功能；  5.支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、Mysql、MSSQL、DB2、Oracle、HTTPS、SMTPS、POP3S、IMAPS等协议报文（HTTPS、SMTPS、POP3S、IMAPS加密协议解析需要导入服务器私钥证书），并提供审计协议类型的端口号配置，可根据需要变更端口号；支持LDAP登录行为识别；支持VXLAN镜像流量解析检测；  ★6.支持检测WEB攻击、异常访问、恶意文件攻击、远程控制、WEB后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼、邮件恶意链接、DGA域名请求、SMB远程溢出攻击、WEB行为分析、隐蔽信道通信、暴力破解（包括SSH、TELNET、RDP、FTP暴力破解）、挖矿等风险（提供截图证明）；  7.支持对私网地址IP地理位置信息添加，在产生告警时，定义IP可正常显示所属地理位置信息；  8.可支持详细展现告警级别、时间、威胁名称、状态、客户端IP、客户端IP所在地理位置、服务端IP、服务端IP所在地理位置、报文、操作等信息，包含请求URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie、请求参数、响应码、返回长度等信息。  9.可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等；  10.对基于木马回连的非法数据传输等行为进行取证分析，包括回连主机IP、服务器IP、传输数据大小、协议类型等。  ★11.支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等，可显示一句话类webshell后门是否植入成功（提供截图证明）；  12.自动关联行为分析的详细展现，包含SQL注入取数据、表单破解、XSS测试、目录穿越读取文件、多人访问Webshell、APT攻击等。  ★13.支持场景化的分析能力，对发现的告警进行二次关联，支持对勒索病毒、网站后门、邮件APT攻击等事件进行预警。（提供截图证明并加盖原厂商鲜章）；  14.支持HTTP、FTP、SMB、SMTP、POP3、IMAP、HTTPS、SMTPS、POP3S、IMAPS等协议传输文件检测；  15.支持kafka、短信、邮件、syslog、snmp、ftp等告警方式；  ★16.动态沙箱检测：动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险，可展示文件中版本信息、段信息、资源信息、导入表、字符串信息、删除文件信息等内容（提供截图证明并加盖原厂商鲜章）。  ★17.支持根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机host和完整沙箱分析报告；（提供截图证明并加盖原厂商鲜章）；  ★18.支持根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机host和完整沙箱分析报告（提供截图证明并加盖原厂商鲜章）；  ★19.支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、同步验证、信息收集等功能。（（提供截图证明并加盖原厂商鲜章）；  20.具备软件著作权证书、销售许可证（必须是APT安全检测类）、ISCCC增强级认证证书" |
| 10 | 接入层交换机 | 3台 | 24口千兆交换机 |
| 11 | 服务器内存扩容 | 1批 | 3台服务器物理内存扩容至64GB。 |
| 12 | 防病毒软件扩店 | 50个点 | ★防病毒软件扩点，满足终端安全需求。需要与医院现有防病毒软件兼容，能使用同一个控制中心进行管理。（提供截图证明并加盖原厂商鲜章） |
| 13 | 安防子系统 | 1套 | 包含门禁控制器、门禁读卡、门禁控制软件、电磁锁、镀锌线管及信号线 |
| 14 | 机房消防系统 | 1套 | 包含柜式火装置、紧急启停按钮、声光报警器、感温探测器、感烟探测器、灭火器、其它辅助材料及人工 |
| 15 | 数据中心网络整改 | 1次 | 对数据中心网络布线按照等保要求进行铺设，对网络布局按照等保要求进行整改。（包含网线及水晶头） |

# 为保证有效的原厂服务，本次项目不接受OEM产品，不接受贴标产品。

**备注：**

**1.论证文件费和专家评审费由中标人支付。**