**数据库审计系统招标技术规格书**

**一、工程说明**

随着集团公司的业务的发展，业务应用和网络使用对信息安全的保障要求越来越高，集团公司共有安全监测、人员定位、矿井三维、ERP、外网网站五个业务系统进行了等级保护测评，其中ERP系统须符合等级保护三级标准要求，其他四个业务系统须符合等级保护二级标准要求，根据《信息系统安全等级保护基本要求》（GB/T22239-2008），集团公司对定级的信息系统需要进行基本的安全等级保护。在等保相关控制点能够满足的条件下，尽量加强防护水平，实现安全的信息系统为集团公司的生产提供可靠的保障。

**二、设备采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 单位 | 数量 | 主要参数 | 备注 |
| 1 | 数据库审计系统 | 台 | 2 | 网络端口：支持监听接口扩展； 1个电口管理口；支持千兆网络环境下的监听能力， 6个以上千兆电口网络接口；4个以上千兆光口。  系统自带内部存储，存储空间不低于2TB，支持RAID0/RAID5；支持外部存储设备。  采用专用工控机硬件架构，非普通PC服务器，保证稳定可靠。  旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计。  支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL等多种主流数据库审计；  SQL语句处理能力：>=24000条SQL每秒  检索能力：10亿条日志的数据规模，查询响应时间<8秒。  支持主流业务协议 HTTP、Telnet、FTP、SMTP、POP3、DCOM；  支持数据库操作类、表、视图、索引、存储过程等各种对象的所有SQL操作审计；  支持基于数据库访问日期、时间、源/目的IP、来源、数据库名、数据库表名、字段值、数据库登陆账号、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计功能及审计查询功能；  支持数据库请求和返回的双向审计  支持对超长SQL操作语句审计，可以正常记录单条长度<=64K个字节的SQL语句内容；  内置安全特征库规则不少于300条，支持对数据库安全进行检查，如SQL注入，缓冲区溢出，数据库漏洞、弱口令等。  支持根据单个数据库或逻辑数据库组、数据库访问行为及按照源IP地址、客户端工具、帐号、告警数等源信息生成报表。  支持热插拔的冗余双电源。 | 三年7\*24原厂保修，出具原厂盖章的服务承诺函 |

**三、设备技术指标**

**1、设备安装说明**

本次所购设备中所有安装材料均按最终现场工勘确认，所需材料均由中标方提供，施工工艺必须满足神华宁煤信息技术中心机房质量标准化标准。设备安装调试所必须的，但本方案中未提及的辅材，例如通过旁路部署利用交换机端口镜像方式获取网络流量的设备需额外配置千兆交换机等，投标方也应在本次招标中一并提供，如有漏项，后期实施时也应无偿提供。

**2、机房环境**

机房位于银川神华宁煤信息技术中心网络数据机房，采用上走线方式。

**3、设计方案**

根据设备须实现的功能采用不同的方式进行部署，串行部署的设备必须具备bypass功能，旁路部署的设备必须能够识别网内的真实流量，依据流量进行相关策略配置。详细方案设计见《网络安全系统建设项目技术方案》。



**4、数据库审计系统详细技术要求**

|  |  |  |
| --- | --- | --- |
| 类别 | 参数 | 功能与技术描述 |
| 配置要求 | 产品架构 | 软硬件一体化产品，冗余热插拔双电源；冗余热插拔风扇。 |
| 部署方式 | 旁路部署模式。 |
| 管理结构 | B/S架构，采用HTTPS方式远程安全管理，无需安装客户端。 |
| 网络接口 | 1个电口管理口，6个以上千兆电口，4个以上千兆光口。 |
| 数据存储 | 系统自带内部存储，存储空间不低于2TB；支持外部存储设备 |
| 并发访问 | SQL语句处理能力：>=20000条SQL每秒 |
| 检索能力：10亿条日志的数据规模，查询响应时间<10秒 |
| 数据库类型 | 支持的数据库类型 | 支持主流数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL |
| 审计能力 | 审计要素及能力 | 支持数据库操作类、表、视图、索引、存储过程等各种对象的所有SQL操作审计； |
| 支持对操作时间、SQL语句、执行结果、返回结果集、影响行数、执行时长、数据库用户名、实例名、源/目的IP、源/目的端口、源/目的MAC、客户端主机名、客户端程序名称、客户端操作系统用户名、业务主机群、SQL模板、会话ID、事件唯一ID等条件进行审计； |
| 支持对超长SQL操作语句审计，可以正常记录单条长度<=64K个字节的SQL语句内容； |
| 准确审计绑定变量的SQL语句 |
| 支持导入审计关联的账号信息，支持通过IP和账号关联到具体SQL是哪个自然人操作。 |
| 安全审计 | 漏洞攻击、SQL注入检测 | 内置安全特征库规则不少于300条，支持对数据库安全进行检查，如SQL注入，缓冲区溢出，数据库漏洞、弱口令等；； |
| 通过模式匹配的方式对SQL访问进行监测与告警,判断是否为可疑SQL注入；须提供界面截图； |
| 告警能力 | 告警策略 | 支持黑白名单告警策略：白名单对象不告警、黑名单对象告警 |
| 模型分析策略：操作语句为原型，根据获取的内容字段（select）、数据库表名、条件字段、操作频率设定分析策略（黑白名单）； |
| 根据SQL执行结果设定策略； |
| 根据IP、MAC、端口、用户设定告警策略； |
| 响应方式 | 根据不同的安全级别采用不同的响应方式，包括记录、告警； |
| 告警方式包括：邮件、短信、SYSLOG、SNMP； |
| 日志及告警查询 | 信息显示 | 三个纬度的导航：会话维度、操作类型纬度、风险纬度 |
| 审计查询 | 审计结果中包括：告警级别、用户名、事件发生时间、客户端IP、目标数据库IP、操作类型、客户端MAC地址、目标数据库MAC地址、客户端端口号、信息大小、返回状态、结果信息、客户端执行命令等详细信息内容。 |
| 报表统计分析 | 自动生成报表 | 支持定时自动生成报表，并发送到指定邮箱 |
| 统计信息 | 设备需具有丰富的分析功能，如事件分析、告警分析、综合分析、会话统计，须提供界面截图。 |
| 支持根据单个数据库或逻辑数据库组生成报表  报表支持按照等级保护标准要求生成多维度综合报告；  支持按照源IP地址、客户端工具、帐号、告警数等源信息生成报表；  支持按照数据库访问行为生成报表，智能识别帐号的增删、权限变更、密码修改、特权操作等行为；  支持按照时间曲线统计流量、在线用户数、并发会话、DDL操作数、DML操作数、执行量最多的SQL语句等报表； |
| 展现形式 | 提供表格、柱状图、饼状图、折线图等多种展示方式 |
| 报表展示 | 固定报表：告警、操作审计、流量 |
| 自定义报表：定期自动生成生成：日、周、月、季度、年度综合报表。 |
| 导出格式支持：WORD\HTML\PDF\EXCEL |
| 数据维护 | 支持自动清理日志信息 | 达到指定阈值时自动清理日志信息 |
| 阈值、开始清理时间、清理时间周期可配置 |
| 支持手动清理日志信息 | 支持手动清理日志信息 |
| 设备安全性 | 系统自身安全性 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 |
| 资质要求 | 产品资质 | 投标产品应具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，提供有效证书的复印件。 |
| 投标方资质 | 投标方应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全服务一级资质证书。  说明：要求提供有效证书的复印件 |

**四、技术服务**

1、投标方投标时必须有原厂针对本项目授权书原件，售后服务承诺函，无原厂授权书取消投标资格，原厂商直接投标不需要。货到现场必须由原厂工程师验货确认后，方可上架安装。

2、投标方在所做标书内必须提交针对本次设备购置的详细技术方案，必须承诺中标后，在施工前了解神华宁煤集团的网络状况并提交详细的施工组织方案，待方案通过后，严格按照施工组织方案进行施工，不得无故延误工期。

3、投标方必须承诺现场施工期间及售后服务时由有相关证书的工程师安装调试设备，不得派遣无资格证书的人员。

4、投标方必须具有独立的法人资质。投标方必须具有中国信息安全测评中心颁发的信息安全服务一级资质，注册资金在1000万以上，具有三个以上的同类同规模工程业绩。

5、投标方所提供的设备是必须是国产设备，如果设备外包装损坏或设备外壳损坏投标方必须无条件更换设备。

6、投标方对所投产品的扩展能力做详细说明。

7、实施期间，中标方负责系统的综合调试，在系统上线运行一个月内对设备性能进行压力测试，出具满足招标文件要求的性能测试报告。须对一切与合同有关的供货设备及技术接口、技术服务等问题负全部责任。凡与合同设备相连接的其它设备装置及软件，中标方有提供接口和技术配合的义务，所发生的费用已包含在投标报价中，招标方不承担中标价格以外的任何费用。

8、投标方应承诺：合同签订后，如招标方需追加购置合同清单内的设备及其附件，所提供的设备及其附件的价格不高于合同价格。

9、培训

投标方应对招标方指定人员提供系统使用、维护等方面的免费培训,培训所需的培训、交通、食宿等各项费用均由中标方承担，培训的时间招标方和中标方共同商议。详细要求如下：

9.1、在不影响施工进度的情况下，中标方应该在安装调试过程中为招标方的技术人员进行现场培训，使招标方的技术人员掌握设备使用技术。培训时间为2-3天，培训费、场地由中标方解决。

9.2、提供中标设备的原厂培训2人7天培训，往返交通、食宿费、培训费等全部费用由中标方承担。

10、售后服务

1）投标方对所提供的设备应提供原厂保修服务，保修期为3年，保修期从安装上架开机运行时计算。在保修期内，投标方应无偿并迅速更换非人为因素损坏的整机设备和相关配件，并解决因软件及操作等产生的相关问题。

2）投标方应提供保修期以后的维保办法及维保报价。

3）在接到设备故障通知后，投标方应在1小时内做出响应，及时进行提导并提供解决方案，如需要上门维护必须在24小时以内到达现场。