# 技术、商务及其他要求

## 采购清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **单位** | **数量** |
| 1 | 数据库安全审计系统1 | 台 | 1 |
| 2 | 数据库安全审计系统2 | 台 | 1 |

## 技术参数及要求

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **详细技术指标及功能需求** | **备注** |
| **1** | **数据库安全审计系统1** | **基本要求：**1. ★数据库审计设备采用专用的2U机架式独立硬件设备（非Windows平台）；
2. ★国产自主品牌，非OEM产品，提供计算机软件著作权证书复印件并加盖原厂公章鲜章；
3. 所投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》（提供有效证书复印件并加盖原厂公章鲜章）；
4. ★为了方便管理和维护，数据库安全审计系统1和数据库安全审计系统2应该具有保持良好的兼容性；

**配置要求：**1. ★配置不少于1个千兆电口监听口，不少于1个千兆管理口；配置不少于2块2TB硬盘；支持RAID1；支持不少于1个千兆扩展板，双电源；设备最大支持不少于4个千兆监听口；包含嵌入式审计引擎软件1套；
2. ★本次配置不少于13个被审计对象授权，后期根据实际需要可进行扩充；
3. 抓包速度：2000M；库速度:32000条/秒；日处理事件数：10000万条；

功能要求：1. 采用B/S管理方式、无需在被审计系统上安装任何代理；
2. 持透明部署、支持单臂路由、支持路由模式、支持NAT、支持Bypass；
3. 下级控制台（数据中心）可以设置接受上级管理、上级控制台（数据中心）可以查看所有下级的拓扑和状态、上级控制台（数据中心）可以为下级生成报表、上级控制台（数据中心）可以为下级下发审计对象；
4. ★支持Oracle、Informix、DB2、SQL-Server、Sybase、PostgreSQL 、Mysql数据库审计；支持Teradata、Cache 、人大金仓、达梦数据库的审计；（提供截图证明加盖原厂公章鲜章）
5. ★支持网络邻居审计（Netbios协议）、NFS协议审计；（提供截图证明并加盖原厂公章鲜章）
6. 支持Telnet协议、FTP协议、Rlogin协议、Radius协议、RDP协议、SSH协议、SCP协议、SFTP协议的审计；
7. 支持自动方式建立web访问和SQL访问之间的对应关系，生成访问行为模型库；
8. 支持对于模型库以外的未知HTTP操作、未知SQL操作可进行标注审计；
9. 持中间件环境下的SQL语句关联到HTTP操作，HTTP操作关联到HTTP-ID，实现中间件环境下的审计追溯；
10. 支持支持事后关联和实时关联两种方式；
11. 支持对针对数据库的XSS攻击行为进行审计；
12. 支持对针对数据库的SQL注入攻击行为进行审计、提供对数据库返回码的知识库和实时说明，帮助管理员快速对返回码进行识别；
13. 支持数据库并发会话数、并发进程数、并发用户数、并发游标数、并发事务数、数据库锁等超过限制的审计；
14. 支持数据库绑定变量审计、支持SQL操作响应时间的审计、支持Select操作返回行数的审计；
15. ★支持审计NFS协议的用户名、文件名等、支持审计Radius协议的认证用户MAC、认证用户名、认证IP、NAS服务器IP；（提供截图证明并加盖原厂公章鲜章）
16. 支持按数据库名、数据库表名、字段值、数据库登陆账号、数据库操作命令、数据库返回码、SQL响应时间、数据库返回行数作为查询和统计条件；
17. 审计系统上存在大量敏感信息，必须对审计管理员进行强度更高的认证，管理员登陆支持硬件令牌认证；
18. ★支持SNMP方式，提供系统运行状态给第三方网管系统；支持NTP时间同步；（提供截图证明并加盖原厂公章鲜章）。
 |  |
| **2** | **数据库安全审计系统2** | **基本要求：**1. ★设备应为2U专用硬件，配置专用安全操作系统，不应采用软件+x86服务器结构；
2. ★国产品牌，提供计算机软件著作权登记证书有效复印件加盖原厂公章鲜章；
3. 投标人所投产品须获得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》，提供有效证书复印件并加盖原厂公章鲜章；
4. ★为了方便管理和维护，数据库安全审计系统1和数据库安全审计系统2应该具有保持良好的兼容性；
5. 要求为配置一和配置二的设备实现数据流量的复制与聚合，能够对多路输入流量进行输出复制、分发、汇聚；

**配置要求：**1. ★系统具备不少于6个数据采集口，支持Console口管理，系统有效存储容量不少于2TB；本次配置不少于130个审计对象授权；能够平均每秒采集入库3000条事件；内置双电源模块；
2. 流量复制与聚合模块配置不少于8个千兆电口，不少于2个SFP千兆光口，不少于4个XE万兆口，具备LCD液晶屏，内置双电源模块；
3. 系统必须采用B/S架构，管理员只需浏览器即可连接到系统进行各种操作。
4. ★产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护；
5. 产品应具备客户端浏览器兼容性，至少支持IE与Firefox；
6. ★系统必须采用基于浏览器的用户界面，至少支持IE与Firefox。界面布局简洁，操作方便；为了适应不同用途，用户可以对界面颜色进行选择调整；

**功能要求：**1. ★支持对数据库、网络设备、安全设备和系统、主机操作系统以及各种应用系统的日志、事件、告警等安全信息进行全面的审计；
2. ★无需另外安装软件组件，审计中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、NetBIOS、OPSEC等多种方式完成日志收集功能；可灵活定制不支持的数据源采集，而无须改动代码；
3. 允许用户安装独立的日志采集器通过上述方式采集日志并转发给审计中心；
4. 允许用户在被采集节点上安装日志代理采集日志并转发给日志采集器或者审计中心；
5. 审计中心可以支持多个日志采集器；
6. 系统提供基于资产的拓扑视图，可以按默认，略图和详图三种模式显示资产拓扑节点；
7. 拓扑视图可以显示被审计资产之间的网络连接关系。用户可以手工编辑拓扑，包括添加节点，添加/编辑连线，任意拖动节点，可以对拓扑图进行缩放，可以更换拓扑图背景；
8. 用户可以随意在资产的拓扑图和列表视图之间进行切换；
9. 在资产管理界面可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表；
10. 系统必须具备日志范式化功能，实现对异构日志格式的统一化；
11. 范式化字段至少应包括事件接收时间 、事件产生时间、事件持续时间、用户名称、源地址、源MAC地址、源端口、操作、目的地址 、目的MAC地址、目的端口、事件名称、事件摘要 、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等；
12. 传输数据具备加密压缩传输能力，保证数据的完整性和机密性；
13. ★支持加密压缩方式转发，定时转发；（提供截图证明并加盖原厂公章鲜章）
14. 支持对信息的自动合并，减少数据数量，节约存储空间；
15. ★可以建立日志合并条件，设定合并的时间范围。（提供截图证明并加盖原厂公章鲜章）
16. ★支持以SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、NetBIOS、OPSEC等多种方式完成日志收集；
17. 系统允许管理员实时的，以监视场景的形式查看不同类型的日志信息；
18. 用户可自定义监视场景，每个监视场景都要以监视策略的形式进行存储，并形成一个监视树；
19. 实时显示日志内容包括：接收时间、事件类型、事件名称、报警级别、来源IP、目的IP、设备类型、设备来源IP等；可查看日志详细信息和原始信息；
20. 可以显示一段时间的动态日志移动图，能够在图上显示每个时间切片的日志数量、等级，并能够在图上显示总的事件数和每秒事件数。用户点击每个时间切片，可以查看该切片内的日志；
21. 系统允许管理员以统计场景的形式查看不同类型的日志信息；
22. ★可对日志分析视图进行随意推拽缩小或放大日志分析时间段，系统会实根据选中的时段时刷新展示该时段内的日志（提供截图证明并加盖原厂公章鲜章）
23. ★支持支持对日志进行柱图、饼图、堆积图、时间轴图、等级堆积图、折线图、折柱混合图等形式进行可视化的展示；（提供截图证明并加盖原厂公章鲜章）
24. ★用户可自定义查询条件，并以策略保存，并以树形结构进行组织，形成一个查询树；（提供截图证明并加盖原厂公章鲜章）
25. ★系统在复杂查询条件（两个查询条件）下查询性能不低于5000万条记录/秒。（提供截图证明并加盖原厂公章鲜章）
26. 系统具有日志关联分析的能力，能够对不同的日志进行相关性分析，发掘潜在的信息；
27. ★系统可实现统计计数关联，能够设定一段时间内的事件发生次数的阈值，还能指定重复事件的属性特征（提供截图证明并加盖原厂公章鲜章）
28. 日志告警：告警动作支持告警重定义、弹出提示框、发送邮件、发送SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送MSN、发送Syslog等方式；告警内容可以自定义，可以根据日志的实际情况将参数传递给命令行脚本；告警可查询，导入导出；
29. 日志报表：提供内置报表模板；支持按照天、月度、季度、年度等时间周期生成报表；支持在报表中以柱状图、曲线图、饼状图方式统计安全报警情况；支持报表报告的导出，导出的格式支持EXCEL、PDF、DOC、XML、HTML、RTF等，支持Office 2007格式；系统内置报表编辑器，可以自定义报表；
30. ★系统管理：可以对自身运行的CPU、内存和磁盘空间等的使用率设置告警阈值（提供截图证明并加盖原厂公章鲜章）
31. 用户管理：实现基于角色的权限管理；要求系统管理员、权限管理员和用户管理员三权分立；系统内置上述三类管理员；
32. 要求同时支持复制和汇聚模式，实现对检测流量的复制、汇聚：

1)实现1路到N路复制（N小于32）、N->N路复制以及支持分组流量复制；2)支持N路到1路汇聚、支持N->N路汇聚、支持分组流量汇聚；33、★流量取证模式：不改变目标交换机配置情况下，设备任意口接入网络，其他网络接口作为镜像模式进行流量取证，分析。 |  |

## 项目履约时间、地点

**履约时间：**合同签订后30天内交货；

**履约地点：**西南交通大学犀浦校区图书馆。

## 付款方式

1.分期付款，第一期，合同签署后支付合同总额的60%；第二期，货到验收合格，在中标人支付招标人5%的质保金后十个工作日内，招标人支付合同总额的40%；第三期，正常运行一年后退还质保金；

2.成交人需提供增值税普通发票。

## 服务要求

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求项目** | **服务要求标准** |
| 1 | 服务要求 | 1、技术文件：应提供全套、完整的书面技术资料，包括设备说明书、操作手册、简单维修说明等。2、设备安装、调试和验收：在合同生效后应向用户提供详细的安装要求并提供技术咨询；在设备到达前，供应商应通知用户水、电、气及其他设备等必备辅助设施的具体要求，从而让用户提前做好设备安装准备。设备到达用户所在地，在接到用户通知后一周内进行安装调试，直至通过验收。3、技术培训：在用户所在地对设备使用者进行设备操作和维护进行培训，使被培训人员达到能够熟练使用。培训内容包括设备的技术原理、操作、数据处理、基本维护等，同时面向用户免费提供不少于1人次的注册信息安全专业人员（CISP）和2人次CCNA(或同等级)认证培训和考试。★4、保修期：提供设备原厂5年7\*24小时 免费质保服务，包括但是不限于配件更换服务、人工服务、设备调优服务、原厂工程师到场服务等，提供设备原厂厂商针对此项目的5年售后服务承诺函原件，保修期自仪器验收签字之日起计算。保修期间设备维修及零件更换费用由供应商负担。5、维修响应时间：保修期内，在收到用户的维修服务要求后2小时内做出回应，4小时内到达用户现场进行维修，应使仪器恢复正常使用。6、软件升级：应免费向用户提供在硬件许可条件下的软件升级服务。 |
| 2 | 售后服务承诺 | 投标人提供完善的售后服务方案，对项目售后服务内容的合理性、全面性进行综合比较评分。 |
| 3 | 服务标准 | ★投标产品质保：设备硬件质保期为5年，软件系统维护期为5年。 |
| 4 | 备品备件 | 投标人提供的备品备件方案完善、合理且具有针对性 |
| 5 | 服务体系 | 技术支持与服务体系健全，组织机构、管理和服务人员针对工程实际配置且合理。  |
| 6 | 响应速度 | 投标人故障现场服务时间要求：4小时内到达服务现场。服务现场2小时内解决技术故障，24小时内提供备品备件服务。 |
| 7 | 人员资格 | 投标人项目实施人员的学历、职称、资质认证等说明，并提供有效的证明材料； |
| 8 | 培训 | 投标人培训方案的完整性，包括内容、人员、时间、地点、频次等。 |
| 9 | 集成实施服务 | 投标人要根据本项目特点，提供集成实施和安装施工调试方案，负责本次所有投标产品的安装调试集成等服务工作，费用包含在投标总价中。 |

注：服务要求中加★号指标为关键指标，不满足将导致投标被拒绝。