|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络安全设备 | 序号 | 商品名称 | 数量 | 控制总价（元） |
| 1 | 防火墙设备 | 2台 | 120000.00 |
| 2 | 日志综合分析平台 | 1台 | 90000.00 |
| 3 | 数据库安全评估系统 | 1台 | 90000.00 |

**玉环市档案局局域网网络安全设备的在线询价**

1防火墙设备技术参数要求：

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **功能描述** |
| ★设备性能要求 | 专有硬件平台 | 硬件采用MIPS多核处理架构，多核核数≥2个 |
| 接口数量 | 设备高度≤1U，≥9个10/100/1000M自适应电口，每个接口可划分到不同安全域实现各接口间的安全隔离，1个USB接口 |
| 电源 | 单电源，可选双冗余电源 |
| 设备性能 | 最大吞吐量≥1Gbps，IPSEC VPN≥600Mbps,最大并发连接数≥40万，每秒新建连接≥1.2万， |
| 网络适应性 | NAT功能 | 支持NAT扩展技术，突破传统单个公网IP地址64512个端口的瓶颈达到更大值（要求提供界面截图） |
| 支持NAT地址可用性探测，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 |
| 路由协议 | 支持静态路由、等价路由、策略路由，以及BGP、RIPv1/v2、OSPF、ISIS等动态IPv4路由协议（非透传），策略路由支持基于指定IP地址、指定应用协议、指定时间表生效 |
| IPV6协议 | 基本功能 | 支持DHCPv6 ,静态路由、策略路由、RIPng、OSPFv3等 ipv6协议，（提供产品功能截图有效） |
| 支持隧道、DNS64/NAT64等多种过渡技术， |
| 安全功能 | 支持IPv6应用识别，访问控制，IPS攻击防护，防病毒，（提供产品功能截图有效） |
| 监控功能 | 支持IPv6用户的流量，会话，新建，应用监控统计集，（提供产品功能截图有效） |
| 支持查看IPS,AV,攻击防护等IPv6威胁日志功能，  |
| 支持IPv6日志存储及标准syslog server。 |
| 防火墙 | 抗DDoS攻击 | 支持抵御所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood等，动作支持记录、阻断两种模式（必须具备攻击防护软件自主知识产权证明） |
| ARP防护欺骗 | 为了防御ARP攻击和ARP病毒，支持免费 ARP广播及ARP客户端认证，本次招标要求配置1000台客户端授权。提供软、硬件协同防御ARP欺骗的界面截图或技术文档做证明（提供产品功能截图有效） |
| 策略管理 | 支持防火墙策略命中数统计和策略的冗余性检查功能,便于管理员维护防火墙策略（提供产品功能截图有效） |
| 应用协议智能识别 | 支持Windows、Android、IOS平台3000+种的应用识别及控制 |
| 支持自定义应用及应用组,应用特征库支持网络实时更新 |
| 负载均衡 | 链路负载 | 支持SmartDNS功能；注：SMARTDNS功能实现当外部用户访问内部服务器时，联通用户解析到的域名IP为联通地址，电信用户解析到的域名IP为电信地址（提供产品功能截图有效） |
| 支持就近探测算法（根据SYN报文探测的响应时间和PING报文探测的响应时间等方法自动生成静态路由表，并将探测的响应时间生成日志）选择最优路径（要求提供界面截图） |
| 支持基于链路使用率和时延进行链路切换，提升出口的访问效率（提供产品功能截图有效） |
| 服务器负载功能 | 支持服务器的负载均衡，提供加权轮询、加权最小连接数、加权散列等多种负载均衡方式（提供产品功能截图有效） |
| 管理功能 | 系统回滚 | 支持2个系统软件并存，并可在WEB界面上直接配置启动顺序，防止配置不当或系统故障造成的网络中断，充分保证系统的稳定性，支持不少于10个配置文件并存，并支持回滚。（提供产品功能截图有效） |
| 云端SaaS管理平台对接  | 支持通过云端SaaS管理平台为用户提供便捷、高质量以及低成本的增值安全服务，要求通过手机 APP能够实时监控防火墙等设备的状态、网络流量、威胁等信息，及时获得告警，并提供丰富的报表和日志托管能力（提供产品功能截图有效） |
| 终端接入监控 | 支持跨三层识别接入网络终端数，支持识别Windows、IOS、Android等9种操作系统 |
| 支持IP、管控规则、接入终端数、状态等条件过滤查询监控结果 |
| 支持对超限IP进行日志记录、干扰操作，禁止共享接入（提供产品功能截图有效） |
| 用户认证 | 支持微信连wifi认证，无需输入用户名密码进行一键认证，完成认证后可以上网（提供产品功能截图有效） |
| 支持基于支持本地用户，Web认证，短信认证，MAC认证， |
| 产品资质要求 | 销售许可证 | 具备计算机信息系统安全专用产品销售许可证（千兆增强级） |
| CVE认证 | 具有下一代防火墙产品的CVE兼容性证书（非IPS产品） |
| 产品成熟度 | 连续五年入选过Gartner企业防火墙魔力象限，提供证明文件 |
| 信息安全产品认证证书 | 具备《中国国家信息安全产品认证证书》（千兆三级） |
| NSS LAB认证 | 下一代防火墙产品获得NSS LAB推荐级别认证，提供证明文件 |
| 防雷击 | 防雷击浪涌等级三级以上，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 |
| MAPP成员 | 要求加入微软安全响应中心发起的MAPP计划，作为该计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护并提供微软官网截图 |
| 其他要求 | 中标后测试 | 中标人在中标后7个工作日内需提供样机测试，并进行所承诺的所有功能测试，提供测试报告，如经测试发现与标书要求或投标文件不一致或投标单位有意拖延测试，则视为欺诈行为，招标人将不授予合同，投标单位将承担一切后果与责任 |
| 原厂服务 | 签订合同前提供原厂3年售后服务承诺函 |

1. 日志审计技术参数要求：

|  |  |  |
| --- | --- | --- |
| 指标名称 | 指标项 | 详细描述 |
| 资质要求 | ▲产品资质 | 1. 提供产品的《计算机软件著作权登记证书》
2. 国家公安部计算机信息系统安全专用产品销售许可证；
3. 通过国家保密局涉密信息系统产品认证；
 |
| 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； |
| ▲产品架构 | 采用标准**1U机架式硬件**，深度定制化Linux Kernel+Busybox，系统独立运行在1024M的SD卡中，系统运行不依赖于硬盘【提供原厂盖章页面截图】 |
| 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 | 1. 所供系统设备必须自带本地存储功能；
2. 提供基于海量日志专用存储的文件系统著作权证书，禁止采用通用关系型数据库来存储日志；
3. 物理磁盘空间：2\*1TB；硬盘支持热插拔；
4. 日志存储数量10亿条
5. RAID架构以保证数据可靠性,
 |
| ▲存储扩展 | 1. 支持扩展外部网络存储(IP SAN、NAS、DAS、磁盘阵列等)；
2. 支持云备份存储模块；支持天翼云、阿里云、百度云、腾讯云、华为云、沃云、移动云、亚马逊云等多家云存储供应商接口
 |
| ▲网络接口 | 2个千兆电口； |
| 授权许可 | 支持50个日志采集源数量许可 |
| 处理性能 | 日志采集能力：3000条/秒以上 |
| 功能要求 | 日志数据采集类型 | 1. 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[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神]、AS400日志、 [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]；
2. 支持SNMP日志采集，支持日志类型：网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神]
3. 支持Opsec Lea日志采集；（提供产品页面截图证明）
	* 内置数据库审计模块；通过流量镜像协议解析；支持DB2、Oracle、MSSQL，MYSQL、Informix、SyBase数据库各版本的访问行为审计；【提供原厂盖章产品页面截图证明】
4. 支持文件传输模块[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；
5. 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；
	* 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；【提供原厂盖章产品页面截图证明】
6. 审计系统支持以syslog、snmp trap、opsec lea、WMI等标准协议接口采集各类日志数据；
7. 审计系统自动将采集的操作语句解析为查询、增改、删除、过程等类型呈现；
8. 审计记录包括行为发生时间、员工工号、操作终端主机名及IP地址、终端工具名称、服务器端主机名及IP地址、数据库名、表名、SQL语句、返回结果等关键信息。
	* 提供工号信息接口，将数据库操作语句与操作者工号建立关联关系，实现操作者实名认证；【提供原厂盖章产品页面截图证明】
	* 审计系统能够对未经许可的客户端工具直接访问数据库的行为实施阻断；【提供原厂盖章产品页面截图证明】
9. 支持配置操作行为解析模型（黑白名单），灵活区别正常操作和异常操作事件；
10. 支持依据语句解析模型，以操作频率为条件实施行为阻断；
11. 支持将可疑的数据库查询语句以在线的方式反显执行，并即时在线查看返回结果；
12. 支持将异常操作的完整会话信息进行前后操作语句关联查看分析；
13. 支持分中心部署方式，能够配置分支数据集中上传至中心机；
 |
|  |
| 基本功能 | 监控功能 | 1. 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；
2. 支持自定义配置实时监控的日志类型；
3. 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；
4. 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；
5. 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 | 1. 系统内置多种类报表模板；
2. 支持动态\静态（日报、周报、月报）两种系统生成方式；
3. 支持报告的邮件转发、生成提醒功能；支持多人邮件接收；
4. 支持自定义审计报告；
5. 支持导出html、Excel、PDF；
6. 支持管理员自定义审计报表模板；
 |
| 查询分析功能 | 1. ▲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；【提供原厂盖章产品页面截图证明】
2. 支持以日志类型、时间范围及条件字段快速检索过滤；
3. 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；
4. 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；
5. 支持查询模版创建、修改、删除功能；
6. 支持查询结果导出；
7. ▲支持海量日志数据高性能查询分析行为审计分析引擎，【提供原厂盖章的相关国家级产品技术证明】
 |
| 策略管理功能 | 1. 支持内置归并策略，对HTTP数据进行自动归并处理；
2. 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；
3. 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）
4. 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；
5. 规则条件设定支持逻辑运算符与支持正则表达式；
6. ▲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；（提供原厂盖章产品页面截图证明）
7. 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 | 1. 支持按日志属性、日志类型、时间范围等进行数据备份；（提供产品页面截图证明）
2. 支持WEB界面备份及日志恢复导入工作；
3. 支持自动与手动两种备份归档方式；
4. 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；
 |
| 系统配置功能 | 1. 支持审计系统用户（组）管理（添加、修改、删除、停用、启用）；
2. 支持资产管理，即所有采集日志源管理维护；
3. 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；
4. 支持证书页面生成下载；
5. 支持系统配置备份恢复；
6. 支持时间同步页面配置；
7. 支持页面方式系统升级以及设备关闭、重启；
8. 支持从WEB界面查看网卡IP设置，修改静态路由设置等内容；
9. 支持安全页面（SSL）证书下载；
 |
| 系统安全 | 系统自身安全 | 1. 系统内置安全防火墙；支持控制访问审计主机范围；
2. 必需提供内部通讯检查机制，传输128加密；
3. 管理接口支持串口或电口的方式管理；
4. 管理界面与其他功能模块分离；
 |
| 日志数据安全 | 1. 审计日志文件方式存储；
2. 审计日志加密导出审计系统；
3. 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 | 1. 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）
2. 支持日志类型、IP地址权限设置；
3. 支持页面功能模块权限设置；
 |
| 系统许可方式 | 永久许可方式，再增加审计用户的情况下不用增加授权许可； |
| 产品授权及服务 | 提供针对本项目的原厂授权函；提供原厂三年7\*24小时的售后服务承诺； |

1. 数据库安全评估系统技术参数要求：

|  |  |
| --- | --- |
| **技术参数** | **指标** |
|  漏洞库 | 漏洞数 | ≧2800条（提供产品截图证明） |
| 漏洞类别 | ≧10种 |
| 检测点 | ≧5800（提供产品截图证明） |
| 遵循标准 | ★支持国际漏洞库CVE和国家漏洞库CNNVD，产品生产厂商应具备数据库漏洞挖掘能力，提供已挖掘且得到CVE和CNNVD确认的数据库危险漏洞编号并提供原创漏洞证明（官方截图或证书），至少提交国外和国内的数据库漏洞各3个。 |
| 质量要求 | ★产品开发质量管理体系符合GB/T 19001-2016/ISO 9001:2015和GB/T22080 -2016/ISO/IEC 27001:2013标准，符合专业数据库安全系统的设计开发和服务标准认证，提供认证证书。 |
| 00 | 风险等级 | 应包括高、中、低、警告等不同等级 |
|  检测能力  | 检测对象 | **★**应支持Oracle、SQL Server、DB2、MySQL、SyBase、Postgres、Informix等7种国际主流数据库，应支持DM、KingBase、GBase 三种国产数据库（提供产品截图证明） |
| 检测范围 | **★**应包括缺省口令、弱口令、低安全配置、DBMS脆弱点、补丁漏洞、程序后门、易受攻击代码等类别（提供产品截图证明） |
| 检测方式 | **★**应支持授权扫描、渗透测试方式（提供产品截图证明） |
| 渗透检测 | **★**应支持弱口令检测、SQL注入检测、缓冲区溢出等方式检测（请提供产品截图证明） |
| 弱口令 | **★**可按穷举、字典库、规则等多种方式，不受数据库尝试登陆次数的影响（提供产品截图证明），其中DM6和DM7的8位以里密码的口令穷举破解，不超过1分钟。 |
| 端口识别与发现 | 能够自动发现、准确识别出网络中正在运行的数据库服务； |
| 报告分析 | 报告格式 | 应支持html、doc 、pdf格式 |
| 报告类型 | 支持综合报告、风险点检测报告、详细检测报告等类型；详细报告中应包含漏洞的来源、CVE/CNNVD编号、风险级别、漏洞类型、漏洞描述、修复方法等详细内容 |
| 支持弱口令、高危程序等单项报告 |
| 支持对比分析、趋势分析等统计分析报告 |
|  增强功能  | 监控能力 | 应能对数据库运维安全状况的监控,包括用户、权限信息、连接信息。 |
| 敏感数据发现 | 能根据用户的特点和要求，自动化完成系统内所有敏感数据项的汇总。 |
| 宽泛权限扫描 | 可对系统内所有用户和授权情况进行扫描，为用户提供权限是否宽泛的判断依据。 |
| 可扩展口令库 | **★**应允许扩展弱口令检查的字典库,用户可以指定专门的库文件。（提供产品截图证明） |
|  管理功能 | 用户管理 | 应提供系统管理员、扫描操作员、审计管理员三权分立功能 |
| 任务管理 | 应允许每个任务中包含一个或多个目标数据库，用户可以自定义扫描的各项参数、扫描策略、任务名称和描述。 |
| 应能对已执行任务的结果进行保存，可以集中查看。 |
| 审计管理 | 可以对管理员、操作员的各种行为进行审计；对检测结果可按照时间、数据库配置信息等进行审计分析。 |
| 升级管理 | 应支持本地手动升级。 |
|  策略管理  | 预定义扫描策略 | 支持全面扫描、CVE漏洞扫描、CVNNVD扫描等类型策略； |
| 支持缺省配置、危险程序、敏感数据等单项扫描策略； |
| **★**支持等保专用检测策略(含2级、3级，同时覆盖各种主流数据库)（提供截图证明。） |
| 自定义策略 | 用户可以根据自己的行业特征和关心的安全点，有针对性地建立检测项集合,形成行业检测策略。 |
|  安全性  | 检测用户权限 | **★**使用只读权限的数据库账户，即可完成全部检测内容。 |
| 漏洞库保密 | 支持漏洞库采用加密方式进行保护，防止对漏洞库进行篡改，导致检测结果的失效，以及对数据库造成破坏导致业务系统运行受到严重损失。 |
| 检测结果保密 | **★**支持对检测报告信息采用加密技术，避免IP、端口等配置信息，弱口令等重要内容泄密（提供截图证明。） |
| 系统危害性 | 不对系统的任何参数、数据变更，不发生任何写操作相关的行为。 |
| 产品资质 | 产品具有中华人民共和国国家版权局《计算机软件著作权登记证书》。产品具有公安部销售许可证。产品具有国家保密科技测评中心《涉密信息系统产品检测证书》。 |
| 公司资质 | 原厂商应为国家信息安全漏洞库技术支撑单位。原厂商应为商用密码产品生产单位并具有商用密码产品销售许可证。原厂商应为网络安全应急服务支持单位证书。 |