## 采购项目商务和技术要求

|  |  |  |  |
| --- | --- | --- | --- |
| 技术要求 | | | |
| 序号 | 技术和性能参数名称 | 招标参数和性能要求 | 备注 |
| 1 | 基本要求 | 1.采购防火墙5台  2.采购入侵防御设备1台  3.采购入侵检测设备1台  4.采购日志分析设备1台 | 不接受负偏离 |
| 1.1 | 技术力量 | 一、投标产品应具有以下证书： 1.要求所投产品具备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公章。 •2.防火墙要求所投产品具备IT产品信息安全认证证书EAL4增强级，提供有效证书复印件并加盖公章。 3.防火墙要求所投产品具备由中国信息安全测评中心颁发的国家信息安全漏洞库CNNVD兼容性资质证书，提供有效证书复印件并加盖公章。 4.入侵检测和入侵防御产品应具备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公章。 •5.入侵检测和入侵防御产品应具备信息安全产品认证证书，提供有效证书复印件并加盖公章。 •6.日志审计具有中国国家信息安全产品认证证书（增强级），提供有效证书复印件并加盖公章。 二、投标方人员力量： 为保证本项目的服务质量，需为本项目配备1名项目经理，2名实施工程师。投标方所有项目人员需具备本公司近半年的社保证明。 1.项目经理应掌握项目管理体系知识及经验，需具备项目管理体系知识认证PMP证书； •2.项目经理应拥有良好的沟通能力，具备培训讲师或咨询师经历，具备CISP信息安全专业人员认证。 3.实施工程师需具备CISP注册信息安全专业人员认证。 |  |
| 2 | 2.1防火墙产品功能及要求 | 1.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 •2.支持对二层协议进行访问控制。 3.支持BGP、RIP、OSPF等动态路由协议。 4.支持NAT穿透技术ALG，支持FTP、TFTP、SQLNET、PPTP、RTSP、SIP、H.323等协议。 •5. 产品支持IPSec VPN智能选路功能 6. 产品支持应用管控功能和多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略。 •7. 产品支持对压缩病毒文件进行检测和拦截，压缩层数支持12层及以上。 8. 产品支持对HTTP、FTP、POP3、SMTP等协议进行病毒防御。 9. 支持与入侵检测设备连动，根据入侵检测设备传送的连动信息，防火墙自动生成拦截策略进行拦截 10. 支持网页浏览、论坛发帖、电子邮件、即时通讯、文件传输、服务器操作等信息关键字的实时检测和过滤。 11. 针对事件关联分析，可以提供多种入口，比如基于应用、目的IP、源IP、用户、攻击事件等。 •12. 产品内置不低于8000种漏洞规则。 •13. 支持SNMPV1/V2/V3/Trap等标准网络管理协议。 14. 支持管理员三权分立功能，根据管理员权限分为安全管理员、安全审计员、系统管理员三种角色。 15. 支持多次登陆失败后锁定IP或锁定用户功能。 •16. 支持通过本地帐号/Radius进行用户身份识别。 \*17.标准机架式设备，双电源，内存≧8G，接口≧4千兆电口+2万兆光口SFP+ \*18.网络层吞吐量≧20G，应用层吞吐量≧9G，防病毒吞吐量≧1.5G，IPS吞吐量≧1G，全威胁吞吐量≧1G，并发连接数≧200万 |  |
|  | 2.2入侵防御产品功能及要求 | 1. 支持路由模式、旁路部署、单臂部署等多种方式； 2. 系统须支持802.1Q VLAN Trunk、access接口类型，VLAN三层接口和子接口； 3. 系统特征库数量7000条以上。 •4. 系统须提供规则升级更新内容。 •5. 系统应内置海量URL分类库。 6. 系统应能识别主流的应用程序，识别不少于6000个应用。 •7. 系统应支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、地域、认证用户等因素实现对象的流量控制。 8. 支持策略导入导出功能。 9. 支持安全策略一体化配置，通过一条策略快速实现不同安全功能的配置，简化策略配置工作； 10. 支持本地密码认证，LDAP、Radius等服务器外部密码认证 •11.系统应支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、地域、认证用户等因素实现对象的流量控制。 12. 支持根据起始时间、结束时间、源IP、目的IP等多种条件快速进行安全日志查询，支持按照不同风险级别查询不同日志； 13. 报表输出格式需支持多种格式。 14. 系统应提供多种升级方式 \*15.标准机架式设备，双电源，内存≧4G，接口≧4千兆电口+2万兆光口SFP+ \*16.网络层吞吐量≧5Gbps，IPS吞吐量≧500Mbps，并发连接数≧150万，新建连接数≧5万 |  |
|  | 2.3入侵检测产品功能及要求 | 1. 支持路由模式、旁路部署、单臂部署等多种方式； 2. 支持链路聚合功能，可将多条物理链路聚合成一条带宽更高的逻辑链路使用 •3. 系统攻击特征库数量7000条以上 4. 支持连接会话展示，可针对IP地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体IP的会话记录； •5. 系统应能识别主流的应用程序，识别不少于3000个应用。 6. 支持Land、Smurf、WinNuke、Tear Drop、IP数据块分片传输、超大ICMP数据攻击等攻击基于数据包攻击防护；支持IP协议异常报文检测和TCP协议异常报文检测。 7. 支持根据起始时间、结束时间、源IP等多种条件快速进行安全日志查询，支持按照不同风险级别查询不同日志； 8. 报表输出格式需支持多种格式。 9. 支持内置规则库的手动与自动更新。 10. 系统同时能提供CPU利用率、内存利用率、会话状态、流量状态、风扇状态、板卡状态等监控信息展示。 \*11.标准机架式设备，内存≥8G，接口≧4千兆电口+2万兆光口SFP+ \*12.网络层吞吐量≧20Gbps，并发连接数≧200万，每秒新建连接数≧15万； |  |
|  | 2.4日志分析 | 1. 支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、FTP、等多种方式完成日志收集； 2. 日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量 3. 支持日志文件备份到外置存储节点，支持以FTP方式将日志数据备份至外部存储空间； •4. 支持将检索查询的条件收藏为查询模版，支持查询模版创建、导入导出、删除功能，支持历史搜索记录功能。 5. 支持自定义审计规则。 •6. 支持设置日志存储策略，包括设置日志存储周期（天）、存储空间容量使用阈值等。 7. 系统应内置丰富的事件规则，应支持自定义事件规则 8. 包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。 9. 提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持只允许某些IP登录平台；支持页面权限配置 •10. 支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。 \*11.标准机架式设备，内存≧16G，硬盘容量≧4T，接口≧4千兆电口+2万兆光口SFP+ \*12.主机审计许可证书数量≧50，平均每秒处理日志数（eps）最大性能≧2000 |  |
| 3 | 附加验收条件 | 通过系统全流程运行测试，运行检测时间≥1个月。 |  |
| **\*商务要求(均为实质性响应条款，不接受负偏离）** | | | |
| 1 | 交货时间 | 合同签订后1个月内安装调试完毕,具备运行条件 |  |
| 2 | 交货地点 | 北京市海淀区 |  |
| 3 | 付款条件 | 签订合同物资到货验收合格后付95%，验收合格满一年后付5% |  |
| 4 | 售后服务 | 1.软硬件设备待项目验收后免费维保及软件升级≥3年； 2.服务期内出现紧急故障情况，公司应在收到服务请求后30分钟内响应，4个小时内到现场，12个小时内解决问题，12小时内无法解决的硬件问题应及时提供相应的备用设备，提供7×24小时热线电话支持服务，负责提供技术问题的解答和技术指导； 3.无专用维修工具，可提供维护使用手册； 4.原厂提供不少于3日的设备使用培训； 5.提供原厂售后服务承诺函及授权； 6.每年不少于4次的巡检服务并提供巡检报告，提供维修及配件服务，提供软件免费升级和维护。 |  |
| **备注：1.商务条款及基本要求不接受负偏离。**  **2.加注“\*”、“.”号的技术指标均需提供证明材料。**  **3.供应商须提供相关技术指标证明材料予以佐证（证明材料不限于资质证书、业绩案例、响应承诺，以及产品规格表、制造商官方网站发布的产品信息、说明书等或检测机构出具的检测报告等技术资料支持的、产品彩页、技术白皮书、厂家出具的技术证明文件、实物照片、软件功能截图等）。** | | | |