第五章 采购项目技术、服务、政府采购合同内容条款及其他商务要求

**前提：本章采购需求中标注“\*”号的条款为本次磋商采购项目的实质性要求，供应商应全部满足。**

## 一、项目概述

本项目为网络安全等级保护三级安全建设项目，共1个包。

## 二、项目清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **标的名称** | **数量** | **单位** | **所属行业** |
| 1 | 防火墙 | 1 | 台 | 工业 |
| 2 | 数据库审计 | 1 | 台 | 工业 |
| 3 | 堡垒机 | 1 | 台 | 工业 |
| 4 | 全网行为管理 | 1 | 台 | 工业 |
| 5 | 日志审计 | 1 | 台 | 工业 |
| 6 | 备份一体机 | 1 | 台 | 工业 |
| 7 | 安全服务 | 3 | 年 | 软件和信息技术服务业 |

## 三、商务要求

\*1、完成时间

在合同签订后30个工作日内完成安装并通过验收，若无法按时完成，采购人有权单方面退货并追究成交供应商的违约责任（提供承诺函原件并加盖公章）。

\*2、质保期

本项目自竣工验收之日起提供为期三年的质保期。

\*3、其他要求

（1）项目实施期内，投标人至少派驻1名项目经理在采购人指定地点配合实施本项目。项目经理原则上不能更换，更换实施人员须征得采购人书面同意。

（2）机房网络安全等级保护三级解决方案建设中须提供机房现有业务系统迁移服务：一是硬件设备的检测。在迁移以前，对现有的设备进行一次全面的检测，包括系统状态、组件和系统配置的检测，确认系统迁移恢复后应具有的功能和性能。二是配合业务系统的开发维护单位，协调网络供应商、软件开发公司进行设备检测，确认系统迁移恢复后应具有的功能和集成方式；做好数据备份工作，对各系统配置参数和配置文件做有效的记录和保存，为系统再运行、集成提供充分的依据。三是暂停业务系统服务，设备停机断电下架。四是搬迁至新机柜上架加电开机业务系统重新启动。

\*4、交货及验收

4.1供应商交货期限为合同签订生效后的 25个工作日内交货到采购人指定地点，随即在5个工作日内全部完成安装调试验收合格交付使用 (如由于采购人的原因造成合同延迟签订或验收的，时间顺延)。交货验收时，采购人有权要求提供产品质检部门从同类产品中抽样检查合格的检测报告。

4.2验收标准：按国家有关规定以及磋商文件的质量要求和技术指标、供应商的响应文件及承诺与本合同约定标准进行验收；双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由采购人在磋商文件与响应文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收。

4.3如质量验收合格，双方签署质量验收报告。

\*5、付款方式

5.1采购人在本合同签订后收到发票之日起 5个工作日内支付合同金额百分之50%的价款；

5.2全部货物安装调试完毕并验收合格之日起，采购人接到供应商通知与票据凭证资料以后的30日内，向供应商核拨合同总价50%的尾款。

\*6、售后服务

成交供应商在接到采购人故障通知后应在10分钟内电话响应，2小时内指派工程师（设备制造商认证的服务工程师）抵达现场，进行检测、维修；24小时内不能解决必须提供备用设备，如货物经成交供应商3次维修仍不能达到合同约定的质量标准，视作成交供应商未能按时交货，采购人有权追究中标人的违约责任。

成交供应商须承诺所有货物必须是全新原厂原装未拆封正品，成交后提供的产品配置与响应文件响应的配置一致。（提供承诺函。）

## 四、技术、服务要求

|  |  |  |
| --- | --- | --- |
| **序号** | **产品名称** | **技术参数** |
| 1 | 防火墙 | \*1.性能参数：网络层吞吐量≥12G，应用层吞吐量≥4G，并发连接数≥200万，HTTP新建连接数≥8万，IPSec最大隧道数≥1000，  硬件参数：内存大小≥8G，硬盘容量≥64G minisata SSD，接口：千兆电口≥6个，千兆光口≥2个；  ▲2.产品采用多核并行处理架构（提供第三方国家认可的合法检测机构出具的关于“多核并行安全操作系统”的证书或测试报告）；  3.产品具备静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议；  ▲4.为防止网页遭到恶意攻击，产品需支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用；（提供相关功能截图证明）  5. 支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护；  ▲6.为防止勒索攻击，产品能够支持勒索软件通信防护功能（提供第三方国家认可的合法检测机构出具的关于“勒索软件通信防护”产品功能检测报告；  7.产品具备文件过滤功能，可对视频文件、音频文件、图片文件、文本文件、可执行文件、驱动文件等类型文件进行安全过滤；  ▲8. 具备基于国家/地区的流量管理功能（提供第三方国家认可的合法检测机构出具的关于“国家/地区的流量管理”产品功能检测报告；  9.设备安全日志支持本机存储、Syslog服务器存储、态势感知平台存储等不同形式存储方式；  10. 支持内容敏感数据防泄露功能，对传输的文件和内容进行检测,支持对银行卡号、手机号码等类型数据防护；  ▲11.支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞；（提供相关功能截图证明）  12. 产品内置安全报表模板，可定义报表内容，包括网络整体安全状况、服务器安全风险分析、终端主机安全分析等；  13. 安全规则库支持在线自动升级、手动升级、云端实时升级等多种方式。   \*14. 供应商需提供产品的由中国网络安全审查技术与认证中心（中国信息安全认证中心）按国家标准认证颁发的有效认证证书 |
| 2 | 数据库审计 | \*1.性能参数：吞吐量≥3Gbps，SQL处理性能≥30000条SQL/s，日志检索性能≥1亿条日志， 硬件参数：内存大小≥8G，硬盘容量≥2TB SATA，接口：千兆电口≥6个，千兆光口≥2个；  ▲2.支持数据库连接工具白名单功能，自动忽略数据库连接工具访问数据库的默认操作（提供相关功能截图证明） ；  3.支持以源IP、业务主机、操作类型、SQL模版、数据库用户为维度的数据库行为排行；  4.支持集中管理，可集中管理多台审计设备审计事件的存储、分析，实现统一配置、统一报表、统一查询；  5.支持内置高风险规则，防范维护人员执行no where 删除、truncate table等合法的授权的高危操作检测；  ▲6.产品能够基于访问的时间、次数、访问客户端IP、客户端操作系统主机名、客户端操作系统用户名、客户端连接工具名、数据库用户名、数据库IP、数据库实例、表、列等、操作类型、执行成功、执行失败、执行时长、返回行数、登录成功、登录失败、SQL异常、SQL模式、SQL关键字等；（提供相关功能截图证明）  7. 提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能；  ▲8.产品能够以曲线连接多点的形式展示用户的访问来源、目标、操作的轨迹；（提供相关功能截图证明）  9.支持Syslog告警、SNMP trap告警、邮件告警，短信告警等多种告警方式；  ▲10.为了方便统一管理，要求所投产品与防火墙为同一品牌。 |
| 3 | 堡垒机 | \*1.性能参数：运维授权数≥50，图形运维最大并发数≥100，字符运维最大并发数≥200，硬件参数：内存大小≥4G，硬盘容量≥1T SATA，接口：千兆电口≥6个；  2.用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式；  3.支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入 ；  4.支持Windows AD域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号；  ▲5.内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴；（提供相关功能截图证明）  6.支持RDP安全模式（RDP、NLA、TLS、ANY）设置，以适应RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高；  7.支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问；  ▲8.支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批；（提供相关功能截图证明）  9.支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯；  10. 全面支持Windows、linux、国产麒麟系统、Android、IOS、Mac OS等客户端操作系统下的H5页面一站式运维，实现跨终端适应性BYOD（Bring Your Own Device）；  11. 需支持HA，配置信息实时同步，配置过程在web界面完成；  12. 具有日志防溢出功能，当磁盘空间达到阈值时，可设置停止记录审计日志或日志回滚；  13. 全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计；  ▲14.支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行，命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人。（提供相关功能截图证明） |
| 4 | 全网行为管理 | \*1. 性能参数：网络层吞吐量≥5Gb，应用层吞吐量≥750Mb，带宽性能≥500Mb，支持用户数≥4000，准入终端数≥2000，每秒新建连接数≥10000，最大并发连接数≥500000，硬件参数：内存大小≥4G，硬盘容量≥1T SATA，接口：千兆电口≥6个，千兆光口≥2个；  ▲2.产品配置web界面提供分析显示接入用户人数、终端类型、认证方式、带宽质量分析、实时流量排名、泄密风险、违规访问、共享上网等行为风险情况；（提供相关功能截图证明）  3．同一个账号，支持与指定数量的多个终端进行自动绑定；  ▲4.支持拨号行为、双网卡行为、有4G网卡、有无线网卡行为、连接非法wifi行为、使用非法网关行为、连接外网行为、自定义外联行为，8种外联方式的检查；（提供相关功能截图证明）  ▲5.支持通过抑制P2P的上行流量，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；（提供相关功能截图证明）  6.支持二维码认证，管理员扫描访客的二维码后对其网络访问授权；  7.针对SSL加密的网站、论坛发帖、web邮箱的内容进行关键字过滤和内容审计；  8.支持检测windows重要补丁的安装情况，并反馈检测结果，支持IP管理功能，管理员可以查看每个IP的详细使用情况。 |
| 5 | 日志审计 | \*1.性能参数：主机审计许可证书数量≥50，可用存储量≥1TB，平均每秒处理日志数（eps）最大性能≥1200；  2.支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件；  ▲3.支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射；（提供相关功能截图证明）  4.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IP免登录，指定IP免认证直接进入平台；支持只允许某些IP登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；  5.支持个性化定制，支持全系统更换logo与系统名称，支持一键恢复默认；  ▲6.支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；（提供相关功能截图证明）  7.支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka等多种方式完成日志收集；  ▲8.支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括base64、Unicode、GBK、HEX、UTF-8等；（提供相关功能截图证明）  9.支持自定义审计规则与关联规则，支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上；  ▲10.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；（提供相关功能截图证明）  11.支持日志文件备份到外置存储节点，支持NFS、NAS、ISCSI三种存储方式，并可查看外置存储容量、状态等信息。 |
| 6 | 备份一体机 | 1.基本要求：管理操作界面需采用中文，软件安装配置应简单容易；具备简便、直观和友好的图形操作管理界面，备份/恢复有图形进度显示；能满足分布网络集中式管理的需求；  2.规格：≤2U机架式  3.处理器配置：8核处理器≥1，可扩展至双处理器；  4.缓存： 1GB缓存，最大支持不小于1TB；  5.系统盘：≥480G SSD固态硬盘；  6.主机接口： 2个1Gb千兆主机接口,可扩展到不小于8个，并支持万兆主机接口、8G FC、16G FC接口扩展；  7.容量扩展：容量可无缝扩展至600TB以上，并支持扩展柜；  \*8. 备份功能：本次配置≥16TB裸容量，提供客户端应用数据备份许可，不限应用端数量；  9.风扇、电源：双冗余、热插拔电源和风扇；  10.备份功能：多个备份任务可以并行同时执行；备份软件对所有已备份数据和磁带介质的管理应简单高效，备份数据列表可以快速查找和浏览；应具备详尽的历史日志记录、查询、管理和报告功能；能提供容灾备份/恢复、重删功能；  11.基于时间的镜像恢复技术：要求在界面上，支持通过设置时间深度，可瞬间显示过去或现在的任意时间点文件系统的镜像，可快速查找或恢复被删除文件；  12.兼容性：支持Windows、Linux、麒麟、红旗等多种操作系统；支持Oracle、SQL Server、DB2、Sybase、Mysql、达梦等各类系统平台数据库备份,SAP、Exchange等应用文件备份，操作系统快速备份等, 虚拟机环境支持Vmware、Hyper-V，XENServer主流版本、ICS5.5等；备份一体机生产厂商通过Openstack认证，发布Cinder驱动并合入Openstack社区的主干版本中；  13.数据库及应用备份：支持K-DB、SQL、Oracle、DB2、Lotus Notes、Sybase 、Mysql、Exchange、Active Directory、SharePoint、Enterprise Vault以及部分国产数据库及应用备份；  14.灾难恢复能力：备份管理须具有灾难恢复能力，可以在发生极端灾难时迅速地通过灾难恢复磁带将整个系统迅速恢复，无需重新安装操作系统、驱动程序、应用系统等等，支持源端重删功能，降低网络压力。 |
| 7 | 安全服务 | \*1、服务内容:安全运维服务  服务要求：机房安全巡检；至少包含机房环境、网络设备状态、安全设备状态、应用系统状态等的检查与分析，了解采购人当前系统与设备的运行情况，并对发现的安全隐患提供改善建议，并出具安全巡检报告。  服务期限：3年（每季度一次） |