**招标项目技术、服务、商务及其他要求**

（注：当采购包的评标方法为综合评分法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

（注：当采购包的评标方法为最低评标价法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。）

**3.1采购项目概况**

本次采购的防火墙分别部署在统计专网陕西节点中互联网出口区、统计业务区和办公区等相关区域，按照统计专网设计架构及相关文件精神，按照品牌异构原则构建统计专网安全防护体系，不同区域的网络安全防护设备须配置为不同品牌，建成品牌差异化的统计网络安全架构，强化统计专网的稳健性及抗风险性，进一步提升统计专网防御攻击的能力及水平。因此，本次采购的数据库防火墙（2套）、出口区防火墙（2套）、业务区防火墙（3套）各为不同品牌,即供应商必须提供3个及以上不同安全厂商生产的防火墙（含数据库防火墙）设备。

**3.2采购内容**

采购包1：

采购包预算金额（元）: 935,200.00

采购包最高限价（元）: 935,200.00

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 标的名称 | 数量 | 标的金额（元） | 计量单位 | 所属行业 | 是否核心产品 | 是否允许进口产品 | 是否属于节能产品 | 是否属于环境标志产品 |
| 1 | 防火墙系统 | 5.00 | 555,600.00 | 套 | 软件和信息技术服务业 | 是 | 否 | 否 | 否 |
| 2 | 数据库防火墙系统 | 2.00 | 379,600.00 | 套 | 软件和信息技术服务业 | 是 | 否 | 否 | 否 |

**3.3技术要求**

采购包1：

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

标的名称：防火墙系统

|  |  |  |
| --- | --- | --- |
| 参数性质 | 序号 | 技术参数与性能指标 |
|  | 1 | 出口区防火墙：  1.品牌:自主研发的国产化品牌，非 OEM，提供软件著作权登记证书。  2.性能:采用国产自主可控CPU，国产化操作系统，网络层吞吐量≥20Gbps，应用层吞吐量≥15Gbps，并发连接数≥800万，每秒新建连接数≥16万，千兆电口≥6个，万兆光口≥4个，内存≥16G，标准1U架构，冗余电源。  3.网络适应性:  3.1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。  3.2产品支持虚拟防火墙功能，支持虚拟防火墙的创建和删除，具备独立的接口、会话管理、应用控制策略、NAT等资源。  3.3产品支持链路连通性检查功能，支持基于3种以上协议对链路连通性进行探测，探测协议至少包括DNS解析、ARP探测、PING和BFD等方式。  3.4产品支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。  ▲3.5访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试（投标时提供功能截图、说明书、检测报告等任意一种）。  ▲4.应用控制:产品支持应用管控功能，应用特征识别库数量大于9000种，产品支持对不同用户和应用的流量进行带宽的差异化管控（投标时提供功能截图、说明书、检测报告等任意一种）。  5.访问控制：  5.1产品支持基于网络区域、网络对象、MAC地址、服务、应用等维度进行访问控制策略设置。  5.2产品支持ftp协议命令控制功能，至少包含delete、rmdir、mkdir、rename、mget、dir、mput、get、put等，保护对外服务不被恶意篡改。  6.安全防护:  6.1产品支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型。  6.2产品内置不低于10000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则（投标时提供功能截图、说明书、检测报告等任意一种）。  ▲6.3产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为（投标时提供功能截图、说明书、检测报告等任意一种）。  ▲6.4产品支持用户账号安全保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生（投标时提供功能截图、说明书、检测报告等任意一种）。  ▲6.5产品内置超过4500种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护（投标时提供功能截图、说明书、检测报告等任意一种）。  ▲7.安全策略管理:产品支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率（投标时提供功能截图、说明书、检测报告等任意一种）。  8.产品运维管理:  8.1产品支持管理员双因子认证，可以通过用户密码和Key等不同方式登陆产品管理界面。  8.2产品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。  8.3支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险（投标时提供功能截图、说明书、检测报告等任意一种）。  8.4产品支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间。  数量：2 |
|  | 2 | 业务区防火墙：  1.品牌:自主研发的国产化品牌，非 OEM，提供软件著作权登记证书。  2.产品形态:软硬一体机。  3.性能参数:采用国产化操作系统及芯片；冗余电源、内存≥32GB、硬盘≥2TB HDD；千兆电口数≥6个，并至少提供2组电口Bypass；千兆光口数≥4个；万兆光口≥4个；空闲接口扩展槽≥2个；设备最大吞吐量≥20Gbps，最大并发连接数≥500万，每秒新建连接数≥50万。  4.部署模式:支持路由模式、交换模式、旁路模式、虚拟网线工作模式（投标时提供功能截图、说明书、检测报告等任意一种）。  5.双机热备:支持双机热备；支持主备模式和主主模式；支持同步配置、运行状态等；支持配置抢占模式（投标时提供功能截图、说明书、检测报告等任意一种）。  ▲6.虚拟系统:支持虚拟系统，每个虚拟系统逻辑上为一个独立的系统，都有独立的系统管理员、独享的资源和独立的配置界面，根管理员可以对虚拟系统进行资源分配。提供证明材料并加盖厂商公章（投标时提供功能截图、说明书、检测报告等任意一种）。  7.IPV6:支持IPV6，支持IPv6入侵防御、病毒防护、Web防护、弱密码防护等安全功能（投标时提供功能截图、说明书、检测报告等任意一种）。  8.VPN:支持IPSec VPN和SSL VPN，其中IPSec VPN的协商方式为IKEv1和IKEv2，SSL VPN的PC客户端支持Windows、macOS等操作系统（投标时提供功能截图、说明书、检测报告等任意一种）。  9.资产指纹库:系统具备资产指纹库功能，可识别主机、防火墙、web中间件等，资产指纹库数量20万条（投标时提供功能截图、说明书、检测报告等任意一种）。  10.安全策略:  10.1支持一体化安全策略，可基于安全域、MAC地址、IP地址、服务、时间、用户、应用等属性，配置防病毒、入侵防御、内容过滤、URL过滤、文件过滤、Web防护、SSL解密、弱密码防护、防暴力破解、会话老化时间等高级访问控制功能（投标时提供功能截图、说明书、检测报告等任意一种）。  ▲10.2提供对控制策略、上网认证策略、带宽策略、策略路由、源NAT等策略的策略分析，可分析并展示问题策略数量以及所占百分比、问题策略详情、策略宽松度分布情况，简化运维工作（投标时提供功能截图、说明书、检测报告等任意一种）。  ▲11.IPS:系统预定义超过11000条主流攻击规则，包含对应IPS规则的级别、防护对象、操作系统、CVE编号等详细信息（投标时提供功能截图、说明书、检测报告等任意一种）。  12.Web防护功能:支持独立的Web防护模块，系统定义超过4500条WAF规则防护功能，支持常规HTTP漏洞、SQL注入、组件、CMS、WebShell和XSS等类型的Web防护；支持HTTP协议的URL、Method、Referer、User-Agent、Cookie、URL-args等字段的等于、不等于、包含、不包含、正则等多种匹配方式的访问控制（投标时提供功能截图、说明书、检测报告等任意一种）。  13.htts防护:支持SSL加密流量解密功能，支持HTTPS、SMTPS、POPS、IMAPS协议加密的流量解密，支持HTTPS流量按域名分类做流量解密。并支持上层内容安全功能查杀和访问控制，如入侵防御，内容过滤等（投标时提供功能截图、说明书、检测报告等任意一种）。  13.弱口令防护:支持Telnet、FTP、IMAP、POP3、SMTP、HTTP协议的弱密码防护，支持预定义弱密码规则和自定义弱密码防护（投标时提供功能截图、说明书、检测报告等任意一种）。  14.威胁情报:提供威胁情报功能，支持通过关键IP、域名、文件HASH在线检索威胁情报并查看威胁详情，并可检测C&C、勒索软件、僵尸网络、挖矿软件、矿池地址等攻击类型（投标时提供功能截图、说明书、检测报告等任意一种）。  ▲15.智能防护:具备不少于2种工作模式，以应对网络流量过大系统资源不足的情况，在普通模式下，安全引擎处理网络报文遇到资源不足时会将报文直接丢弃，会影响网络转发；在智能模式下，安全引擎将尽可能的处理网络报文，但不影响网络转发（投标时提供功能截图、说明书、检测报告等任意一种）。  16.系统升级:支持系统升级失败自动回滚（投标时提供功能截图、说明书、检测报告等任意一种）。  数量：3 |

标的名称：数据库防火墙系统

|  |  |  |
| --- | --- | --- |
| 参数性质 | 序号 | 技术参数与性能指标 |
|  | 1 | 数据库防火墙：  1.品牌：自主研发的国产化品牌，非OEM，具有软件著作权证书 （提供软件著作权证书复印件）。  2.性能参数：2U机架式设备:双电源、≥8 个电口、≥2个扩展槽位、≥32G 内存，≥128G SSD，≥4T 硬盘，采用国产化CPU:≥8核 16 线程，国产化操作系统， ≥2 个万兆光口（含光模块）带 bypass功能。  3.数据库授权数量：数据库实例数≥64个；数据库流量≥200Mbps。  ▲4.支持数据库类型:支持ORACLE、MYSQL、SQLSERVER、DB2、RDS-Mysql、RDS-PG、TDSQL、PostgreSQL、Informix、Impala、ODPS、Hive、MongoDB、oceanbase、Kingbase、Greenplum、Tidb、神通、达梦等主流国外、国产、云数据库（投标时提供功能截图、说明书、检测报告等任意一种）。  5.支持部署模式:支持透明代理、透明代理NAT、透明网桥、反向代理、旁路、路由网关、HA主备、双主模式（投标时提供功能截图、说明书、检测报告等任意一种）。  支持当设备不可用时，自动启用BYPASS功能，避免设备本身影响业务系统。  6.数据源发现功能:  6.1支持按单个IP或IP段发现数据源。  6.2支持敏感数据自动发现和分类分级，并依据数据分类分级的结果，针对不同权限的业务身份提供细粒度的安全管控，具有某个权限的用户只能访问特定级别的数据。  7.运行模式功能:支持学习、模拟、运行三种运行模式：学习模式支持SQL的自学习，识别安全SQL；模拟模式可以模拟真实操作的管控情况。  8.防护策略功能:  ▲8.1内置数据库漏洞虚拟补丁≥1800个，可阻止黑客通过这些漏洞进行攻击提供证明材料（投标时提供功能截图、说明书、检测报告等任意一种）。  8.2支持正常SQL特征及SQL注入特征双重防护，防止SQL注入攻击。  8.3自动学习业务SQL，捕获SQL语法，生成SQL白名单，通过SQL白名单进行访问控制  8.4支持透明代理模式下的可信IP,将加入到可信IP列表中的可信的终端设备IP地址，终端设备与数据库通信的流量将会进行bypass处理。  8.5支持风险响应策略，针对不同信任度的身份和风险等级设置不同的响应行为（通过、告警、阻断行为、阻断连接）  8.6支持对请求频次访问进行控制，超过频次访问的行为进行阻断或拦截，避免数据大量泄漏。  8.7支持多维身份管理，至少支持应用程序名、IP地址、MAC地址、主机名、操作系统账户、数据库账户、数字证书、时间等因素的任意组合，形成新的登陆认证规则（投标时提供功能截图、说明书、检测报告等任意一种）。  8.8支持检测和审计密码猜测行为，通过设置密码猜测次数限制进行防护，当达到密码猜测限制时，锁定猜测终端，支持自动解锁和手工解锁。  ▲8.9支持数据库防漏扫，当特定的漏洞扫描器对数据库进行扫描时，实现防御拦截（投标时提供功能截图、说明书、检测报告等任意一种）。  9.审计功能:  ▲9.1支持SQL命令的细粒度审计和分析，并详细记录管理用户的行为信息，包括该语句执行的时间、机器名、用户名、IP地址、MAC地址、客户端程序名以及SQL语句等信息，对数据库操作进行审计，可对查询，新增，修改，删除等行为进行监控（投标时提供功能截图、说明书、检测报告等任意一种）。  9.2支持对审计事件过滤功能。  10.告警管理功能:支持多种安全响应措施，支持的告警方式包括页面、邮件、短信。  11.系统管理功能:为增加系统管理的安全性、适应性、可维护性，产品需要具备以下的功能：  ▲11.1支持双因子认证，支持短信认证、证书认证。提供证明材料并加盖厂商公章（投标时提供功能截图、说明书、检测报告等任意一种）。  11.2支持系统安全配置如会话锁定、超时退出、密码复杂性管理等安全措施。  11.3系统支持LDAP/AD域对接，通过域账户统一登录。  11.4支持策略中心全部策略、系统配置、资产配置（资产列表信息、数据源部署模式、数据源分组信息、敏感资产信息等）等进行备份与恢复，支持配置恢复功能。  12.安全运营功能:  12.1支持以图形、列表等方式查看告警信息，以列表形式展现的告警信息应当包含告警时间、告警内容、告警等级、用户IP、数据库代理IP、事件等。  12.2支持告警方式，包括页面、邮件、短信、专有钉、钉钉，并且能智能化分析精确识别违规、高风险行为。  13.报表管理:  13.1支持数据库登录事件、访问事件、风险事件、告警事件等报表的生成。  13.2支持按日、周、月等时间周期生成综合报表。  14.风险监测:可以实现24小时监控SQL注入攻击、数据库漏洞攻击、敏感访问、系统运行、流量等信息。  数量：2 |

**3.4商务要求**

**3.4.1交货时间**

采购包1：

合同签订后15个工作日。

**3.4.2交货地点**

采购包1：

甲方指定地点。

**3.4.3支付方式**

采购包1：

一次付清

**3.4.4支付约定**

采购包1： 付款条件说明： 货物交付验收合格及安装调试验收合格交付使用 ，达到付款条件起 30 日内，支付合同总金额的 100.00%。

**3.4.5验收标准和方法**

采购包1：

验收依据： a) 合同文本； b) 招标文件及澄清函、投标文件； c) 国家和行业制定的相应的标准和规范； d) 验收清单。 验收标准： 按招标文件、投标文件及澄清函、项目运行检查情况等综合指标进行验收。各项指标均应符合验收标准及要求。

**3.4.6包装方式及运输**

采购包1：

涉及的商品包装和快递包装，均应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

**3.4.7质量保修范围和保修期**

采购包1：

产品提供五年原厂质保服务及五年系统与特征库升级服务，质保期内免费维修。

**3.4.8违约责任与解决争议的方法**

采购包1：

详见合同条款。

**3.5其他要求**

发布中标结果公告后，中标供应商应及时向采购代理机构 提交一正二副，书籍（胶装）方式装订的盖章的纸质文件，1套电子投标文件（以U盘形式提供，版本为Word、PDF和拓展名为.SXSTF的电子投标文件）送至西安市碑林区含光北路 2 号广丰国际大厦Ⅱ区 806室。