**附件1**

## 申请人报名应提交资料一览表

项目名称：网络安全产品及服务采购项目

项目编号：贸展总采字〔2023〕045号

报价单位（盖章）

| **序号** | **项目** | **内页码** | **报名提交资料要求** | **审核情况** | **备注** |
| --- | --- | --- | --- | --- | --- |
| （此栏不需申请人填写） |
| 1 | 报名申请函（格式一，同以下资料装订为一本，复印件须加盖公章） |  | 原件 |  |  |
| 2 | 企业法定代表人证明书（格式二） |  | 原件 |  |  |
| 3 | 报名代表人的法定代表人授权委托书（格式三） |  | 原件 |  |  |
| 4 | 企业营业执照复印件 |  | 原件备查 |  |  |

注：1.本表附于报名资料内首页，作为报名资料目录

2列表第1、2、3项按附件一格式一、二、三提交。

**格式一**

**报名申请函**

**致：中国对外贸易广州展览有限公司**

按照询比公告的要求，我公司递交有关资料文件。此申请是由\_\_ \_（公司名）以\_\_\_\_\_\_ \_\_\_\_\_\_（姓名）为全权代表身份递交的。

我们理解邀请单位有权拒绝任何申请，而无需承担任何责任。

申请人名称：（盖章）

法定代表人或授权委托人：（签字或盖章）

申请日期：2023年 月 日

所有与本采购有关的函件请发往下列地址：

地址：

电话(手机)：

传真：

电子邮件：

**格式二：**

**法定代表人（责任人）证明书**

（　 ）第　号

　　　　　　　　现任我单位　　　　　职务，为法定代表人（负责人），

特此证明。

有效期限：

附：

法定代表人（负责人）身份证号码：

单位：（盖章）

　　　　　　　　　　　　　　　　　　　年　月　　日

**格式三： 法定代表人（责任人）授权委托书**

（ ）第 号

兹授权 为我方委托代理人，其权限是：

有效期限：

附：身份证号码：

法定代表人（负责人）：（签名或盖章）

授权单位：（盖章）

年 月 日

注：按提供的格式或使用从工商管理部门购买的格式填写

注：1、**须附委托代理人身份证复印件；**

2、法定代表人证明书和法定代表人授权委托书也可以采用工商部门统一印制的格式。

**网络安全产品及服务采购项目**

**用户需求书**

**一、项目概述**

为保证中国对外贸易广州展览有限公司（以下简称“采购人”）顺利通过网络安全等级（二级）保护备案工作（以下简称“二级等保”），采购人将购买一系列安全产品及相关服务。

本项目为“交钥匙工程”。中选人应完成所响应设备的系统集成、上线调试工作和相关配套服务工作，务必使采购人顺利通过二级等保，中选人所提供的所有设备除特定的外接设备外，所有提供的软、硬件(如接口设备、缆线、网线、光纤、标签、软件、控制器等，包括采购文件中未列出而系统实施又必需的软件、硬件)需配齐以构成一套实用系统。中选人在供货或系统集成时出现任何软、硬件遗漏，均必须由中选人提供，中选人软硬件价格均已包含相关的安装实施费用，无需单列咨询、实施、安装、集成等费用，除特别指出的产品或服务外，其余的产品或服务需保证不少于3年质保期技术支持，服务模式为上门服务(含硬件、软件、授权许可、特征库和系统软件版本升级服务等)，且不再另外收取任何维护费用。

本项目最高限价为28万元。要求供应商开具增值税专用发票。

**二、技术服务要求**

**一）总体要求**

1、供应商须对本项目技术服务要求中的所有内容进行整体响应，任何只对其中一部分服务内容进行的响应都被视为无效响应。

2、所投产品必须是同一品牌，技术参数中要求提供的功能截图或说明文档（均为等保整改重要功能），需提供盖章扫描件，原件备查。

3、供应商中选后，应保证所投产品（服务类除外）在合同签订后30天内交付到采购人指定地点。

**二）产品主要参数配置要求及数量**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **配置要求** | **数量及单位** | **价格（最高限价）** |
| 1 | 日志审计与分析管理系统 | 一、品牌要求：华为、华三、深信服等。  二、性能参数：默认包含主机审计许可证书数量≥50，最大可扩展审计主机许可数≥300，可用存储量：≥2TB（RAID1 模式），平均每秒处理日志数（eps）性能≥4500。  三、硬件参数：规格≦2U，内存大小≥16G，硬盘容量≥128G minisata+2T SATA\*2，电源：双电源，接口≥6千兆电口+2万兆光口SFP+。  四、功能细则要求：  1、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。（需提供产品截图证明或说明文档并加盖公章）。  2、支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。  3、支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志。  4、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。（提供产品界面截图或说明文档并加盖公章）。  五、产品资质要求：  1、产品具备IPv6 Ready Logo认证证书和公安部颁发的《计算机信息系统安全专用产品销售许可证》（提供证书复印件并加盖公章）。  2、提供不少于3年上门原厂整机保修（含硬件、软件及许可授权（如有）等），保修期可在原厂公开渠道进行查验。  六、参与询比的产品配置不能低于以上配置参数。 | 1台 | 80000 |
| 2 | 运维堡垒机 | 一、品牌要求：华为、华三、深信服等。  二、性能参数：默认包含运维授权数≥50，最大可扩展资产数≥300，图形运维最大并发数≥200，字符运维最大并发数≥400。  三、硬件参数：规格≦2U，内存大小≥8G，硬盘容量≥2TB SATA，电源：双电源，接口≥6千兆电口+4千兆光口。  四、功能要求：  1、支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作。  2、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。  3、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；并支持各种认证方式和静态口令组合认证。  4、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。（提供产品界面截图或说明文档并加盖公章）。  5、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。  五、产品资质要求：  1、要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务资质和公安部颁发的《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公章）。  2、提供不少于3年上门原厂整机保修（含硬件、软件及许可授权（如有）等），保修期可在原厂公开渠道进行查验。  六、参与询比的产品配置不能低于以上配置参数。 | 1台 | 79000 |
| 3 | Web应用防火墙（WAF） | 一、品牌要求：华为、华三、深信服等。  二、性能参数：网络层吞吐量≥4Gbps，HTTP应用层吞吐量≥200Mbps，HTTP新建连接数≥40000，HTTP并发连接数≥2000000。  三、硬件参数：规格≦2U，内存大小≥4G，硬盘容量≥128GB minisata SSD，电源：双电源，接口≥6千兆电口+2千兆光口SFP。  四、功能要求：  1、支持虚拟网线部署、透明部署、路由部署、旁路镜像等多种部署方式，适应复杂使用环境的接入要求。  2、支持超过6200种防护规则。其中Web应用防护规则超过4900种，Web应用漏洞攻击防护规则超过1300种。支持自定义Web应用防护规则，支持Web防篡改防护规则，通过基于正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等。（提供产品界面截图或说明文档并加盖公章）。  3、支持语义引擎用于检测Web攻击，能针对不同类型的Web攻击如命令注入攻击防护等，单独选择开启或关闭语义引擎检测。  4、支持业务模型学习监督功能，通过智能分析引擎对业务流量进行分析学习，建立用户业务特征模型，解决因WEB应用中因代码不规范和安全检测功能冲突导致的业务误判问题。  5、支持通过被动扫描功能，业务系统进行黑链检测、Webshell检测、漏洞风险检测、配置风险检测、弱口令账户检测。  五、产品资质要求：  1、产品具备“Web应用防护系统”网络关键设备和网络安全专用产品安全认证证书（提供有效证书复印件并加盖公章）。  2、提供不少于3年上门原厂整机保修（含硬件、软件及许可授权（如有）等），保修期可在原厂公开渠道进行查验。  六、参与询比的产品配置不能低于以上配置参数。 | 1台 | 50000 |
| 4 | 终端安全管理系统 | 一、品牌要求：华为、华三、深信服等。  二、提供≥3年10个服务器EDR全部功能使用授权。  三、功能要求：  1、单一管理控制中心可统一管理分别部署在WindowsPC、Windows服务器、Linux服务器以及国产化服务器的客户端软件；用户端支持部署本地及阿里云端。  2、为保障勒索病毒的防御效果，提供勒索病毒整体防护体系入口，直观展示勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数。  3、提高检测的精准度，产品支持威胁情报，支持跳转链接至云端威胁情报中心，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。（提供产品界面截图或说明文档并加盖公章）。  4、支为避免EDR占用过多业务性能，对业务造成摩擦，可通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整EDR的资源占用（CPU、IO等），为业务让出资源。  5、为防止黑客攻击，支持禁止黑客工具启动，包含：冰刃、xuetr、ProcessHacker、PCHunter、火绒剑、Mimikatz的自启动。  6、支持windows服务器RDP远程登录保护，可开启RDP远程登录二次认证，以防止黑客对服务器的入侵。  四、资质要求：  针对本产品提供公安部颁发的《计算机信息系统安全专用产品销售许可证》虚拟化安全防护产品（增强级）资质证书；（提供证书复印件并加盖公章）  五、参与询比的产品配置不能低于以上配置参数。 | 1套 | 6000 |
| 5 | 下一代防火墙（云端） | 一、品牌要求：华为、华三、深信服等。  二、带宽性能≥100Mbps，新建会话/秒（七层）≥30000，并发会话数（七层）≥1500000，含不少于1年的ACL控制、Ipsec VPN、应用管控与流控、入侵防御、僵尸网络检测、网关杀毒等全部功能使用授权及不少于1年的URL库、应用识别库、IPS特征库、僵尸网络防护库、实时漏洞分析识别库和病毒库特征更新。  三、功能要求：  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、产品支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。  3、产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略。  4、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。  5、产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。  6、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。（提供产品功能截图并加盖厂商公章）。  四、产品资质要求：  1、要求所投产品具备IT产品信息安全认证证书EAL4增强级。（提供有效证明材料并加盖公章）。  2、为保证产品的先进性，要求所投产品需最近6年（2017年1月至2022年12月）入围Gartner企业级防火墙魔力象限。（提供有效证明材料并加盖公章）  五、参与询比的产品配置不能低于以上配置参数。 | 1套 | 20000 |
| 6 | 网络应用防火墙（云端WAF） | 一、品牌要求：华为、华三、深信服等。  二、性能参数： HTTP 应用层吞吐量≥50Mbps，HTTP 新建连接数≥8200，HTTP 并发连接数≥15W。 含软件功能永久使用授权及软件（包含Web攻击防护、Web漏洞攻击防护、Web防篡改等针对Web应用的保护功能），规则库更新授权不少于1年（无防护站点数限制）。  三、功能要求：  1、支持反向代理的部署方式，适应复杂使用环境的接入要求。  2、支持超过4900种Web应用防护规则，和超过1200种Web漏洞攻击特征识别规则。  3、支持语义引擎用于检测Web攻击，能针对不同类型的Web攻击如命令注入攻击防护等，单独选择开启或关闭语义引擎检测。产品原生支持BOT防护功能，可过滤机器人自动化流量，非联动其他组件或产品，并支持用户自定义保护阈值。（提供产品功能截图或说明文档并加盖公章）。  4、支持业务模型学习监督功能，通过智能分析引擎对业务流量进行分析学习，建立用户业务特征模型，解决因WEB应用中因代码不规范和安全检测功能冲突导致的业务误判问题。  5、支持每2小时自动获取云端黑客IP，并能在界面上一键进行访问拦截封堵云端黑客IP。  6、支持对业务详情进行展示，包括业务存在关键的风险，可以提供具体的攻击链过程并对攻击进行举证。  四、产品资质要求：  为保证产品的成熟度，所投产品的生产厂商具备云安全成熟度成熟度模型CS-CMMI 5认证。（提供相关证明材料并加盖公章）  五、参与询比的产品配置不能低于以上配置参数。 | 1套 | 29000 |
| 7 | 网络安全等级保护配置服务 | 服务内容：  1、业务资产梳理服务；  2、等保备案材料准备服务；  3、本地安全设备配置服务；  4、云上安全设备等保配置服务；  5、业务系统安全整改咨询服务；  6、等保测评辅导服务；  7、管理制度梳理服务；  8、原有网络进行分区分域改造服务；  9、在核心、汇聚等交换机的接入ACL访问控制配置服务及VLAN划分服务；  10、中选人需针对采购人在二级等保测评问题清单中的内容进行整改指导，整改率不低于80%（其中测评问题清单的高风险项需100%完成整改）。 | 1套 | 16000 |