

采购需求及技术规格要求

总体要求

1. 本项目报投标总价，投标总价包含完成本项目所产生的一切费用，合同履行期间采购人不再追加任何费用，投标人自行考虑报价风险。

2. 下列采购需求中：标注▲的产品为核心产品，中标的核心产品的名称、品牌、规格型号、数量、单价等将予以公布。

一、项目技术需求

（一）技术需求重要性表述

标识重要性	标识符号	代表意思
关键指标项（基础项）	无标识项	有一条不满足的，投标无效。
重要指标项	★	评分项，具体评分细则详见第四章评标方法和标准。

注：无标识项内容投标人须如实响应，如在后期合同履行过程中，发现有虚假响应情况，采购人有权解除合同、不予退还履约保证金、不予支付合同款项，且上报监管部门并追究中标人给采购人带来的一切损失。

（二）建设目标

序号	设备名称	功能参数	单位	数量	所属行业
1	数据中心防火墙	1. 标准机架式设备，≥8 个千兆电口，≥6 个千兆光口，≥6 个万兆光口，≥2 个扩展槽，磁盘空间≥64G SSD，冗余电源。 2. 防火墙吞吐量≥40Gbps，IPS+AV 吞吐量≥20Gbps，并发连接数≥1000 万。 3. 防病毒库、IPS 攻击特征库、应用特征库、威胁情报等升级授权不少于五年。	台	2	工业

		<p>★4. 支持检查数据包的源地址、目的地址、端口号等信息，并根据规则决定是否允许数据包通过。</p> <p>5. 对于内部网络中的不同用户或部门，可以通过防火墙设置不同级别的访问权限。</p>			
2	WEB 应用 防火 墙	<p>1. 标准机架式结构，内存$\geq 16\text{GB}$，硬盘$\geq 1\text{TB}$，千兆电口≥ 8个，千兆光口≥ 6个，万兆光口≥ 6个，扩展槽≥ 1个，可防护站点数≥ 1000个，网络层吞吐$\geq 40\text{G}$，HTTP吞吐$\geq 20\text{G}$，网络并发连接数≥ 400万，HTTP并发连接数≥ 500万，HTTP新建连接数≥ 90000，五年WAF特征库升级。</p> <p>2. 支持各类拒绝服务攻击，包括：Ping of Death、Teardrop、IP分片等。</p> <p>★3. 支持黑白名单配置：设定可信的访问客户端IP（白名单）不受安全策略规则的检测，设定非法的访问客户端IP（黑名单），直接禁止其对任何Web服务器的访问；支持对防护站点设置客户端、URL等方式的白名单策略。</p> <p>4. 系统具备Web访问控制能力，可以对扫描器的扫描行为、爬虫行为、目录遍历行为进行防御。</p> <p>5. 防护各类带宽及资源耗尽型拒绝服务攻击，能够有效识别，并实时对攻击流量进行阻断。</p>	台	2	工业
3	运维 堡垒 机	<p>1. 标准机架式结构，CPU≥ 8核，存储硬盘容量$\geq 4\text{TB}$，千兆电口≥ 2个，万兆光口≥ 2个，冗余电源。</p> <p>2. 资产授权≥ 500个。</p> <p>3. 用户管理：</p> <p>1) 支持用户的批量导入/导出，按用户类型等分组方式，支持用户安全策略功能，如密码锁定次数、密码复杂度、用户有效期等；</p> <p>2) 支持基于角色的权限访问控制，根据用户角色不</p>	套	2	工业

		<p>同，提供不同的功能。角色权限可以细化到最小颗粒度，如查看、创建、更新、删除资产权限；</p> <p>4. 运维方式：提供浏览器访问方式，支持登陆 Linux 和 Windows 资产；</p> <p>5. 安全策略：支持对运维操作会话的实时阻断、日志回放，包括但不限于起止时间、来源用户、来源 IP、目标设备、协议/应用类型等日志内容。</p>			
4	备份一体机	<p>1. 标准机架式结构，CPU\geq96 核，内存\geq512GB，千兆电口\geq4，PCIE 扩展插槽\geq2 个，硬盘总容量\geq64TB，磁盘槽位\geq12 个。</p> <p>2. 数据备份与恢复系统：支持 X86/虚拟机/云主机的整机快照、持续数据保护、分钟级业务恢复重建、数据去重与合并、多级恢复验证，支持 Windows Sever 和 linux 备份代理程序。</p> <p>3. 业务系统的 CDP 保护授权不限，灾备容量授权\geq100T。</p> <p>4. 当需要数据恢复以及业务快速重建时，可按优先级恢复指定分区的数据，可先行启动预先恢复的业务系统后，将剩余数据逐渐恢复。</p> <p>★5. 支持按时间节点编排自动的主机验证计划，无需停止备份任务，按照设定时间节点开启和释放自动化验证主机所需资源，用于第三方运维、检测、比对工具对最新时间点灾备数据进行调用和比对，确保灾难数据和应用环境的有效性、一致性。</p>	套	1	工业
5	数据库审计	<p>1. 规格要求：内存\geq32GB，硬盘\geq4T，万兆光口\geq2 个，GE 管理口\geq2 个，GE 板载接口\geq4 个，数据库实例授权\geq30 个，Agent 探针授权\geq30 个。</p> <p>2. 性能要求：SQL 每秒入库量\geq8000 条/秒、SQL 峰值吞吐量\geq12000 条/秒、在线会话数\geq4000 个。</p>	台	1	软件和信息技术服务业

		<p>3. 部署方式：支持插件；</p> <p>功能要求：</p> <p>1) 审计系统支持运维人员本地登录 Oracle、MySQL、SQL Server、Db2 等数据库服务器后，直接执行的 SQL 操作的审计，不依赖于数据库自身审计功能；</p> <p>2) 支持在审计系统 WEB 界面管理插件，包括：配置、唤醒、挂起、中断、升级、安装、卸载、下载插件；</p> <p>3) 支持以结果数据为内容作为规则判定的条件匹配告警策略；</p> <p>4) 支持对会话进行统计分析，包括但不限于：从访问来源对新建会话、在线会话进行统计，分析失败登录的来源和目的、时间和失败原因等；</p> <p>5) 支持信息异常查询预警机制，包括但不限于：支持网卡异常、分区超限、异常关机 CPU 超限、内存超限、会话超限、吞吐量超限等。</p>			
6	数据库防火墙	<p>1. 标准机架式结构，内存$\geq 32\text{GB}$，硬盘$\geq 4\text{T}$，万兆光口≥ 2 个，GE 管理口≥ 2 个，GE 板载接口≥ 4 个，接口板卡插槽≥ 1 个，数据库实例授权≥ 50 个。</p> <p>2. 性能：需满足数据库峰值吞吐量≥ 9000 条/秒、在线会话数≥ 2000 个的性能要求。</p> <p>3. 支持 Oracle、SQL Server、MySQL、Db2、DM 等国外和国产数据库系统等。</p> <p>4. 提供敏感访问操作行为防护，通过客户端 IP、数据库用户、客户端工具、客户端 MAC、OS 用户、主机名、时间等定义非法访问。</p> <p>★5. 提供查看语句、会话、脱敏等行为审计，可基于客户端 IP、被保护数据库、数据库用户等维度进行分析，支持语句、会话等多维度的检索能力。</p>	台	2	工业
7	日志	1. 磁盘容量 $\geq 10\text{TB}$ ，日志源接入授权数量 ≥ 1000 个，	台	1	软件

	审计设备	<p>千兆电口≥ 2个。</p> <p>2. 支持设备的 CPU、内存、磁盘空间、利用率监控，支持各类型日志磁盘存储占比统计、支持各类型日志接收趋势统计、支持各设备日志接收趋势统计、支持硬盘健康状态及 Raid 状态监控。</p> <p>3. 支持对设备登入、日志清理、威胁日志数量超限进行告警，支持对文本日志、二进制日志根据字段名、操作符等告警规则。</p> <p>4、支持报告生成。</p>			和信息技术服务业
8	服务器杀毒软件	<p>1. 授权数量≥ 300。</p> <p>2. 支持国产操作系统。</p> <p>★3. 具备高危漏洞免疫功能，当无法通过常规官方补丁进行漏洞修复或面临突发高危漏洞时，可通过微补丁先行覆盖漏洞，客户端或管理平台支持展示当前存在的微补丁及对应的 CVE 漏洞信息，可手动开启或关闭每个微补丁的防护状态。</p>	项	1	软件和信息技术服务业
9	▲密码应用一体化系统	<p>1. 采用基于内核的安全隔离技术和虚拟化密码卡硬件支持，支持独立虚拟化镜像，完成密码产品的部署。</p> <p>2. 产品整体要求：1) 标准机架式设备，存储空间$\geq 2\text{TB}$，千兆电口≥ 8；2) 支持虚拟密码机全生命周期管理：虚拟密码机的创建、启动、停止、漂移等；3) 采用虚拟化密码卡，虚拟化密码卡具备 SR-IOV 虚拟化功能，硬件层进行虚拟化，各个虚拟密码卡内密钥硬件层进行隔离，保障虚拟密码机内的密钥安全；4) 支持独立虚拟化镜像。</p> <p>3. 功能模块要求：</p> <p>1) 签名验签功能：A. 提供密码虚拟化签名验签系统镜像，部署在密码应用一体化系统中，使用数字签</p>	套	2	软件和信息技术服务业

		<p>名技术对数据进行加密，以保证数据的完整性和抗抵赖性；B. 支持国密算法和非国密算法，国密算法包含但不限于 SM2、SM3、SM4 等；非国密算法包含但不限于 SHA-256-HMAC、AES、RSA 等；C. 支持多格式签名验签，包含但不限于：Attached 格式签名验签、Detahced 格式签名验签、RAW 格式签名验签；D. 支持弱算法过滤，且可灵活配置，证书黑名单等安全功能；E. 满足（GM/T 0029-2014）《服务器密码机技术规范》、（GM/T 0028-2014）《密码模块安全技术要求》第二级要求；F. 所投产品具备国家密码管理局颁发《商用密码产品认证证书》；</p> <p>2) SSL 应用功能:A. 提供密码虚拟化 SSL 网关镜像，部署在密码应用一体化系统中。使用 SSL 通讯加密技术，保证数据在传输过程中的通道加密，保证客户端到系统，系统到系统之间的通道加密；B. 支持国密 SSL 算法和国际 RSA 算法的单向和双向认证，至少包含以下算法：国密：SM2、SM3、SM4 算法；RSA：RSA 2048；C. 支持 SSL 拦截白名单，只允许通过指定的域名访问特定的 SSL 服务，支持 SSL DDOS 防御等安全功能；D. 支持命令行页面（OS 命令行）无需安装辅助软件即可运行 ping、tcpdump、telnet 等排错命令；E. 所投产品具备国家密码管理局颁发《商用密码产品认证证书》。</p> <p>3) 数据加解密功能：A. 提供密码虚拟化数据加解密系统镜像，部署在密码应用一体化系统中。为业务系统提供密钥管理，数据加、解密服务，以及数据库中敏感数据加密功能；B. 支持 SM2、SM3、SM4 等商用密码算法，支持 MySQL、Oracle 等主流国际数据库，支持达梦、人大金仓等国产数据库；C. 支</p>			
--	--	--	--	--	--

	<p>持对结构化数据和非结构化数据加解密，支持对称密钥和非对称密钥加解密；D. 支持业务代码无需改造，即可完成数据库切面加密和透明加密功能。应用系统程序可通过数据库开发接口，包括但不限于JDBC、ODBC等方式完成加密后数据库连接；E. 所投产品需提供商用密码产品认证证书，达到《密码模块安全技术要求》二级安全要求；</p> <p>4) 密码服务中台功能：A. 提供密码虚拟化密码服务平台系统镜像，部署在密码应用一体化系统中。使用密码中台技术，可以提供标准化统一的密码调用服务和管理服务，对密码资源池设备进行管控、调度；B. 支持统一安全计算服务，提供对称算法、非对称算法、摘要算法等密码算法的综合安全计算服务，保证客户业务数据的完整性、机密性和可用性；C. 具备多算法的安全计算能力，支持国产 SM2、SM3、SM4 等密码常用算法，平台通过国家商用密码管理局认证，具有《商用密码产品认证证书》；D. 提供国密标准规范接口，需提供国密标准规范接口和甲方自定义接口，并配合适配工作；E. 支持国产化环境部署，产品具备与主流国产化中间件、国产化数据库、国产化操作系统等国产化产品的互认证证书；F. 平台至少支持协同签名服务、动态令牌认证服务、签名验签密码服务、数据加解密服务、数据库加密服务、文件加密服务、SSL 网关服务、电子签章密码服务、时间戳密码服务、密钥管理服务密码服务。</p>			
--	---	--	--	--

（三）服务要求

1. 在服务期限内，免费不限次数提供与系统软件供应商的对接服务，包括但不限于：对系统软件供应商针对密评事项提出各类问题的答疑、指导，根据需要

提供及时的测试服务。

2. 在服务期限内，免费不限次数提供关于等级保护、密评各类需求，包括但不限于：安全检查、基线核查、新业务部署配合以及安全策略调整等内容。

3. 本项目实施过程中所需的模块、线缆包含在项目总价内。

4. 本项目所有设备整体验收后提供不少于 5 年的原厂免费质保。

（四）培训要求

1. 提供项目培训计划，中标方须为本项目中涉及的各个部门的管理员及使用人员组织详尽的培训，确保相关人员可以熟练正确的使用系统。

2. 必须为所有被培训人员提供培训用文字资料和讲义等相关用品。

3. 根据用户需要，提供后续培训任务。

（五）实施要求

1. 投标人需提供拥有丰富经验的实施团队完成本次项目实施。

2. 质保期内承诺提供 7*24 小时服务，并配备专业的服务人员。对于系统在使用过程中出现的问题，在 30 分钟内响应。如遇与所供产品有关的重大问题在接用户通知后 1 小时内应赶到现场提供服务，12 小时内应提供详细的应急解决方案，服务完成后，双方签署现场服务记录。因中标人工作延误，造成采购人损失的，中标人负赔偿责任。