**安全设备及安全系统项目需求参数**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **功能参数** | **单位** | **数量** |
| 1 | 数据中心防火墙 | 1、标准机架式设备，≥16个千兆电口，≥6个千兆光口，≥8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、资产管理、威胁情报等升级授权五年。  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。  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。  6、配置设备冗余连接线缆。 | 台 | 2 |
| 2 | WEB应用防火墙 | 1、标准机架式结构，内存≥32GB，硬盘≥1TB，千兆电口≥8个，千兆光口≥16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≥40G，HTTP吞吐≥20G，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。  2、支持各类拒绝服务攻击，包括：Ping of Death、Teardrop、IP分片等。  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。  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。  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。  6、配置设备冗余连接线缆。 | 台 | 2 |
| 3 | 运维堡垒机 | 1、标准机架式结构,CPU≥8 核，SSD 固态硬盘容量≥480G，存储硬盘容量≥4TB，千兆电口≥2个，万兆光口≥2个,冗余电源。  2、资产授权≥500个。  3、用户管理：  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；  2）支持基于角色的权限访问控制，根据用户角色不同，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；  4、运维方式：  提供浏览器访问方式，支持登陆 Linux 和 Windows 资产；  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。  6、两套设备使用主备方式部署，需配置相关连接线缆。 | 套 | 2 |
| 4 | 备份一体机 | 1、标准机架式结构，CPU≥96核，内存≥512GB，千兆电口≥4，PCIE扩展插槽≥2个，硬盘总容量≥64TB，磁盘槽位≥12个；  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WindowsSever和linux备份代理程序；  3、业务系统的CDP保护授权≥4个，容量授权≥100T。  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。  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数据进行调用和比对，确保数据和应用环境的有效性、一致性。 | 套 | 1 |
| 5 | 数据库审计 | 1、规格要求：内存≥32GB，硬盘≥4T，万兆光口≥2个，GE管理口≥2个，GE板载接口≥4个，数据库实例授权及Agent探针授权≥50个；  2、性能要求：SQL每秒入库量≥8000条/秒、SQL峰值吞吐量≥12000条/秒、在线会话数≥4000个；  3、部署方式：支持插件；  功能要求：  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；  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；  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；  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；  5）支持信息异常查询预警机制，包含但不限于：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。 | 台 | 1 |
| 6 | 数据库防火墙 | 1、标准机架式结构，内存≥32GB，硬盘≥4T，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；  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；  3、支持Oracle、SQL Server、MySQL、Db2、DM等国外和国产数据库系统等；  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。  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。  6、配置设备冗余连接线缆。 | 台 | 2 |
| 7 | 日志审计设备 | 1、磁盘容量≥10TB，日志源接入授权数量≥1000个，支持虚拟网卡数量≥2个；  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。  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。  4、支持报告生成。 | 台 | 1 |
| 8 | 服务器杀毒软件 | 1. 授权数量≥300； 2. 支持WINDOWS、LINUX、国产操作系统； 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。 | 项 | 1 |
| 9 | 密码应用一体化服务系统 | 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；  2、产品整体要求：1）标准机架式设备，存储空间≥2TB，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；  3、功能模块要求：  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》；  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》。  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；  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、密钥管理服务等密码服务。 | 套 | 2 |
| 10 | 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，包含但不限于：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，包含但不限于：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5年原厂免费质保。 | 项 | 1 |