**技术参数**

|  |  |
| --- | --- |
| **产品名称** | **参数要求** |
| **疾控报送服务器密码机** | 1.产品规格：高度≥2U；电源≥2个；内存≥8G；硬盘≥4T；千兆网口≥2个。 |
| 2.支持密钥安全产生、安装、存储、使用、销毁以及备份恢复全生命周期的管理，采用由国家密码管理局批准使用的双物理噪声源。 |
| 3.★支持SM4算法的ECB、CBC、OFB、CFB、CTR等模式的数据加密和解密运算；支持基于SM4算法的保留格式加解密。（提供服务器密码机具备CNAS资质的第三方检测机构出具的功能检测报告） |
| 4.消息鉴别码产生和验证：支持基于SM4 算法的 MAC 产生及验证；数据签名/验证：支持 SM2 算法的私钥签名，使用对应的公钥签名验证。 |
| 5.支持设备初始化配置包括密钥产生安装、生成管理员、按照安全机制对密钥安全存储和备份、系统配置、一键检测等功能，保证设备处于正常工作状态。 |
| 6.支持国产密码算法：SM2、SM3、SM4等；支持审计日志的记录，查询和导出功能；支持多方协同签名、多方协同解密功能；支持密钥分散功能。 |
| 7.双机热备：对外可提供高稳定、高性能的服务，支持热备负载功能，支持多 机并行，提供容错功能，当有密码机出现故障时不影响业务运算。 |
| 8.系统支持可视化管理，支持SNMP协议、系统监控、设备硬件及软件的运行状态监测功能，PGP协议签名/验证、加密/解密，支持接口鉴权签名HMAC、MAC；支持PDF签名、验签功能，支持系统日志审计、业务日志保存、业务日志查询等功能。 |
| 9.★对外可提供高稳定、高性能的服务，支持热备负载功能，支持多机并行，提供容错功能，当有密码机出现故障时不影响业务运算。（提供界面截图证明） |
| 10.★产品须符合疾控统一接口API《疾控报送服务器密码机接口API》。 |
| **疾控报送数字证书** | 1.数字证书格式标准遵循x．509v3标准，符合卫生部《卫生系统数字证书格式规范（试行）》；符合卫生部《卫生系统电子认证服务规范（试行）》。 |
| 2.数字证书有效期5年。 |
| 3.★数字证书应与现有传染病网络直报系统采用的证书兼容互认。需提供证明材料和兼容性承诺。 |
| **防火墙软件** | 1.性能参数：网络层吞吐量:4G;应用层吞吐量:2G;防病毒吞吐量:600M;IPS吞吐量:600M;全威胁吞吐量:400M;并发连接数:200W;HTTP新建连接数:4.5W;SSL VPN推荐用户数（单独购买）:100;SSL VPN最大用户数（单独购买）:500;SSL VPN最大理论加密流量（单独购买）:100M;IPSec VPN 最大接入数:800;IPSec VPN吞吐量:500M;规格:1U; 电源:单电源; 接口：6千兆电口;  2.产品具备先进的僵尸主机监测功能，内嵌了一个包含超过128万种僵尸网络特征的数据库，能够精准地识别并拦截主机上任何可疑的外部连接尝试。（需提供产品功能截图证明和具备CMA/CNAS标识的第三方检测报告）  3.产品支持对不少于9000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。（需提供产品功能截图证明和具备CMA/CNAS标识的第三方检测报告）  4.为了提高提高安全性并方便用户进行精细化管理产品应支持基于网络区域、网络对象、MAC地址、服务、应用、域名等维度进行访问控制策略设置。（需提供具备CMA/CNAS标识的第三方检测报告）  5.产品应支持内置漏洞攻击特征规则库数量超过15000条，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C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。（需提供具备CMA/CNAS标识的第三方检测报告）  6.产品支持管控非法、违规网站的访问行为，具备海量的URL分类库。  7.保护用户会话安全预防跨站脚本攻击(XSS)，产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。（需提供产品功能截图证明和具备CMA/CNAS标识的第三方检测报告）。  8.产品支持用户账号全生命周期保护功能，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。  9.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。（需提供产品功能截图证明）  10.支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息；（需提供产品功能截图证明）  11.产品功能提供使用授权及一年规则库更新服务。 |
| **统一端点安全管理系统软件** | 1.支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和终端账户，其中操作系统和监听端口支持从资产和终端两个视角进行统计和展示。  2.产品支持根据统计周期、终端名称、IP地址，补丁信息和漏洞等级等多维度的入侵检测日志，杀毒扫描日志，微隔离日志，基线检查日志的查询和检测。（需提供国家级检测中心所出具的检测报告）  3.产品支持一键式操作对Windows终端组进行合规性检查，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果。（需提供国家级检测中心所出具的检测报告）  4.为保护用户网络安全产品支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具（需提供产品截图证明）  5.支持基于异常行为AI的实时监测，实现文件动态备份，发生勒索事件时，支持自动删除原始文件夹中被加密的文件夹并隔离文件；支持文件恢复密码保护，用户下发文件恢复操作时需要经过认证校验，确保文件恢复操作的合法性。（需提供产品截图证明）  6.未快速找出并定位遭受病毒感染终端产品支持基于威胁情报的病毒特征值全网终端搜索，可定位出全网终端该病毒的感染情况。（需提供国家级检测中心所出具的检测报告）  7.一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果。 |
| **集成服务** | 对项目涉及的软硬件进行调试。 |