**智能文档私有云存储（一期）和SSLVPN网关产品及服务**

**投标参数要求**

本项目包括：智能文档**私有云存储产品1套和SSLVPN网关产品1套**。本项目为整体交钥匙工程，供应商须负责承担所供货物的整体集成、实施及售后服务工作。本项目根据爱数、赛凡、深信服、天融信、网御、亿云厂商综合得出的技术参数要求。

**技术要求：**

**1、智能文档私有云存储产品 1 套（30万元）**

|  |  |  |
| --- | --- | --- |
| 性能参数 | 1. 对称分布式横向拓展集群存储，所有节点功能一致、地位均等、数据均衡分布，无单独元数据服务器（无索引控制器），无须配置单独的管理服务器。 | |
| 1. ★要求至少配置2个一体化设备，组成高可用集群系统，要求每个云存储节点状态无关，任何管理节点的损坏，都不影响系统的对外服务。 | |
| 1. 单个云存储节点具备自适应 1+1 冗余电源；单个云存储节点配置≥32G高速缓存，缓存最大可扩容≥192GB以上，具备≥4个千兆网络接口。 | |
| 1. ★支持网盘软件,该项目包含私有云盘≥500用户（云盘与存储阵列一体，无需单独服务器，只需开通功能即可）。 | |
| 1. ★本次配置云存储节点≥2个。每个云存储节点具备≥12个可热插拔的磁盘槽位。 本次配置≥16块4TB SATA硬盘。 | |
| 1. 基于嵌入式LINUX系统的专用集群存储设备，内部烧录云共享平台服务端软件，自带硬盘存储空间。要求系统采用SSD硬盘存储，不占用RAID存储空间，实现系统与用户数据分离，提高安全性。 | | |
| 1. ▲ 集群采用多副本冗余存储技术，支持副本数≥3。保证每个数据都会通过读写一致性冗余技术确保存放在不同的节点、不同的硬盘上面。任何一个硬盘和节点损坏都不会影响数据完整性。 | | |
| 1. 支持简单易用的纯中文存储管理系统界面。 | | |
| 1. 系统管理员可以通过登陆Web了解整个集群的运转绩效，要求包括在线人数监控、文件分类数量统计、文件操作变化统计，可以提供实时、每日、每月及年度的报表； | | |
| 1. ▲支持个人文档库访问，以个人用户的用户名为文件库名称，为个人用户所有，属于个人私密性和专属性的文档库。支持开启或者关闭个人文档库； | | |
| 1. 支持自定义文档库访问，由系统管理员创建或者普通管理员创建分类、创建文档库并指派所有者，文档库所有者可以为相应组织的成员配置访问权限，这样成员就可以看到相应的文档库资料； | | |
| 1. 支持共享文档，他人共享给我的文档，包括文件或者文件夹，共享的文件和文件夹都是带权限的，共享的文件可以被修改、编辑，而且会自动更新，不是简单的下载副本资料。 | | |
| 1. 支持PC客户端、移动客户端（Android、IOS）、Web访问等。 | | |
| 1. ▲ 支持软WORM归档固化特性，通过对象文件系统层，实现归档电子资料的安全存储，存储后的数据不可被修改，后端通过切片后使用AES265进行高度加密。归档资料需要通过MD5值校验。（提供软件操作界面截图） | | |
| 1. ▲ 系统、用户和电子文档支持密级管理，根据保密要求，分为机密、秘密和非密三级，系统密级决定用户与文档密级范围，系统密级不能向下调整，低密级用户不能访问高密级文件，高密用户不能把高密文件共享给低密用户，密级文件访问均有日志记录。（提供软件操作界面截图） | | |
| 1. 基于所有者对特定文件及文件夹授权共享给指定的人。对于被共享者，可以随时访问和获得最新的文档进行共享协作。 | | |
| 1. ▲基于文档所有者对指定文档配置指定范围可发现，对于访问者，可以通过全文检索找到可以发现的共享文档进行下载使用。（提供软件操作界面截图） | | |
| 1. ▲ 支持基于云存储的全文检索，当用户想找某个文档资料，希望找到某个关键词相近的文档，输入关键词，获取全文检索的结果，支持文件类型、位置范围过滤，搜索结果支持时间排序。（需提供软件操作界面截图） | | |
| 1. 支持文件重复数据删除技术，相同的文件只上传一次，对于重复上传者而言实现文件的秒传。 | | |
| 1. ▲ 支持与Microsoft Office和WPS Office办公软件无缝结合，支持通过插件实线OFFICE办公软件直接操作和保存云端文件，实线企业内部办公业务闭环。（提供插件集成在Office软件界面的截图。） | | |
| 1. 支持把会议资料开启共享，提供二维码，与会者在微信上扫描二维码，可在线预览会议资料，形成无纸化会议。 | | |
| 1. ▲ 文档删除后自动移动至回收站中存放，可还原文件，回收站按文档库分类呈现，且可以支持文件名、删除位置和删除者的搜索，以便更好的找回误删除文件。（需提供软件操作界面截图） | | |
| 1. 系统支持Windows域用户导入管理。系统管理员可导入域用户及域组织结构，并可将域用户与本地用户进行统一管理，执行编辑、修改、删除等操作，且并不影响Windows域中的用户数据。 | | |
| 1. 要求能够支持同时基于文件及文件夹的多级细粒度权限配置，控制用户对文件及文件夹的显示、预览、下载、上传、修改、删除等权限，同时支持对文件的二级所有权限控制，实现所有权限的下放。支持权限有效期，过期后自动回收权限，（需提供软件操作界面截图） | | |
| 1. 支持移动设备远程数据擦除功能和设备禁用功能；当移动设备丢失时，移动端数据会被擦除并强制退出；也可对设备强制禁用。 | | |
| 1. ▲ 完全Windows使用体验，不改变原有用户使用文件资料的习惯，直接在Windows文件夹下面看到云端文件/夹，直接操作云端文件/夹，无需通过单独客户端界面操作；（需提供软件操作界面截图） | | |
| 1. ▲ 支持对指定文档库设置自动同步，且能够对指定目录进行文件同步大小限制，超过设置大小的文件不允许自动同步；可指定不允许自动同步的文件类型，例如视频、图片、PPT等。（需提供软件操作界面截图） | | |
| 1. 支持丰富的审计日志功能，包括系统管理、人员组织授权、文件操作、权限配置、上传下载、文件访问均有日志记录审计，日志可导出，长期归档，不可被篡改、删除。 | | |
| 产品资质要求 | | 投标产品应为国内知名品牌，非OEM产品，一体化设备，设备包含文档云管理软件和云存储硬件。需提供投标产品《计算机软件著作权登记证书》，提供证书复印件。 |
| ▲要求所投产品须通过国家保密局电子文档安全管理类产品涉密认证。提供证书复印件。 |
| 售后服务 | | ★此台新购设备开通3年软件服务和三年硬件质保；要求提供原厂现场设备软件升级及3年7\*24 技术支持服务； |
| 升级服务 | | ★后继升级授权个数费用，不能超过本期授权数的费用；服务期过后的每年售后服务（包括软件服务、软件升级和硬件质保等）的费用不超过中标价的20%。 |

**2、SSLVPN网关产品 1套（10万元）**

|  |  |
| --- | --- |
| **指标** | **规格要求** |
| 性能要求 | ★SSLVPN和IPSECVPN二合一网关一体化硬件设备;网络接口≥4个千兆电口(包含：至少200个SSL接入授权，以及叁年硬件质保和叁年软件服务) |
| 工作模式 | 支持透明、路由、混合模式 |
| 支持完整性 | IPSec VPN、SSL VPN二合一网关，同时支持IPSec VPN和SSLVPN两种VPN协议 |
| 支持终端使用包括Win7、Mac、Linux等操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用； |
| ▲支持Windows Mobile、IPhone OS、Symbian、Android操作系统的智能手机、PDA等移动终端的SSL VPN接入 |
| 易用性 | 支持虚拟门户功能，每个虚拟门户都可以定制不同的登录界面、定制是否使用控件、定制使用哪些功能模块、定制不同的认证方式、定制不同的公告信息等 |
| ▲可支持远程应用发布功能，发布C/S应用客户端界面而非整个桌面进行发布：只传输鼠标、键盘操作和显示数据，无需安装客户端即可支持C/S模式软件系统的远程使用。SSL VPN不限制远程应用发布的服务器并发。 （需提供截图证明文件） |
| 支持单点登录功能（SSO）,支持移动用户登录VPN后再登录内部B/S、C/S应用系统时不需要二次重复认证。支持HTTP401认证单点登录，支持用户修改单点登陆的账户信息，支持WEB方式的单点登录。 |
| 终端安全 | ▲支持沙盒功能，强制受保护的指定资源仅可在安全桌面下使用；安全桌面下默认仅可与SSLVPN通信，断开互联网链接；在安全桌面内默认禁止外网和本地局域网通讯，禁止和本机默认桌面的通信，防止使用包括USB口设备、打印机等外设的信息外泄。退出安全桌面后清除安全桌面内一切操作和遗留的痕迹，保证重要应用使用的安全性。安全桌面根据用户需要自行配置按用户组、单独用户启用；可配置安全桌面下可访问的指定网段；可配置允许使用COM端口、允许使用打印机、允许与切换到默认桌面、允许本地通信。（需提供截图证明文件） |
| 支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问 |
| ▲支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统（需提供截图证明文件） |
| 身份认证 | 产品必须支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、CA等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行LDAP、USB KEY、硬件特征码、短信认证或动态令牌的四因素捆绑认证 |
| ▲支持短信认证，可自定义所发送短信信息格式，可结合短信猫自行搭建SSLVPN短信认证平台 |
| 智能终端远程应用发布 | 支持Windows Mobile PDA客户端，支持iOS、Android系统的智能终端客户端，支持WindowsXP、2003、2008、2012、Vista、Win7、Win8、Win10、Linux等主流系统。 |
| 支持基于用户、用户组的流量控制和会话限制、无流量超时时间、账号过期时间、闲置失效时间设置 |
| 稳定性、可扩展性 | ▲支持不依赖于第三方的动态IP寻址系统和动态IP组网支持（非DDNS）（需提供截图证明文件） |
| ★支持与原有VPN设备间进行集群（A/A），支持路由模式、单臂模式下多线路部署的集群；支持集群设备间Session同步，一台设备宕机后其上用户无需重新登录SSLVPN可继续使用；可扩展分布式集群功能，无需专门的全局负载设备即可实现异地SSLVPN设备间的接入用户负载分担、速度优选接入，异地设备间互为备份，分布式集群中用户可通过唯一的一个地址访问到所有加入到分布式集群的SSLVPN设备（需提供截图证明文件） |
| IPSec VPN功能 | 总部与分支有多条线路，可在线路间一一进行IPSecVPN隧道建立，并设置主隧道及备份隧道，对主隧道可进行带宽叠加、按包或会话进行流量平均分配，主隧道断开备份隧道自动启用，保证IPSecVPN连接不中断；可为每一分支单独设置不同的多线路策略；单臂部署下同样支持多线路策略（提供自主知识产权证明） |
| 高可用性 | 支持HA功能的主主模式、主从模式；支持链路备份 |
| 防火墙 | 支持强大的访问控制功能，包括安全策略，地址资源，时间资源，服务资源，NAT，端口映射，安全选项等功能 |
| 产品及企业资质 | 设备生产商必须具有高新技术企业证书 (提供复印件) |
| 提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》 |
| ▲提供SSL VPN必须在2008年至今至少曾有一年在中国国内市场占有率为前三名，提供权威的第三方机构数据证明 |
| 产品售后服务 | ★要求原厂商在福建区域设有直属办事处等服务机构，以便于为客户提供完善、及时的售后服务。必须提供7×24小时800电话支持；本地化应急服务紧急攻击事件2小时内响应，最大限度减少损失；提供产品相关的使用和技术培训， |
| 升级服务 | ★后继升级SSL接入授权个数费用，不能超过本期授权数的费用；服务期过后的每年售后服务（包括软件服务、软件升级和硬件质保等）的费用不超过中标价的15%。 |

**说明：**

**(1)全文中带有“**★**”的条款为关键性条款，对这些关键性条款的任何负偏离或不满足将导致投标无效。**

**(2)若招标文件中其它部分的相关条款与技术要求发生理解冲突，则以技术条款解释为准；如发生招标文件的修改，则相关条款以更改通知为准。**

**（3）本文所述技术要求，应视为保证网络运行所需的最低要求，如有遗漏，投标人应予以补充，否则，一旦中标将认为投标人认同遗漏部分并免费提供。**

**评标（综合评分法）**