**附件2：**  **堡垒机采购需求**

**一、招标项目一览表**

具体内容如下表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **标项****序号** | **名称或内容** | **数量** | **单位** | **预算（万元）** | **交货地点** |
| 1 | 堡垒机 | 1 | 套 | 20万 | 仙居县人民医院 |
| VPN设备增加授权 | 1 | 套 |

1. **技术需求**

## 1、堡垒机技术要求

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 性能要求 | ▲配置授权资产≥1000个（最大扩容至2000），并发字符连接最大数≥500个，并发图形连接最大数≥100个 |
| 硬件要求 | ▲2U硬件平台，内存≥8GB，2T硬盘≥2个，千兆电口≥6个，千兆光口≥4个（含千兆SFP多模光模块≥2个），USB接口≥2个，双电源 |

|  |  |
| --- | --- |
| 用户角色 | 支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理；支持自定义用户权限。 |
| 部门层级管理 | 支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；可按部门层级分别设定各部门不同权限的管理员，如部门内的运维管理员、审计管理员、系统管理员等。 |
| 单点登录认证 | ★支持标准化对接CAS、JWT单点登录认证，且支持配置是否自动创建堡垒机中不存在用户（提供产品功能截图） |
| 短信口令认证对接 | ★支持与Get、Post、Soap发送方式的HTTP短信网关平台进行联动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud联动。（提供产品功能截图） |
| 双因子认证 | 堡垒机须内嵌动态令牌和USBkey认证引擎，可使用动态令牌或USBkey进行双因子认证 |
| 密码存储 | ★支持采用国密加密算法进行核心敏感数据加密存储，且支持使用软件/硬件方式加密；（提供产品功能截图） |
| 认证窗口全局设置 | 支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口。 |
| 支持的协议和应用 | 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin、X11；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具 |
| 兼容客户端类型 | ★单点登录支持调用多种本地客户端工具：字符：xshell、secureCRT、putty，图形：mstsc、realvnc，文件传输：secureEX、flashFXP、filezilla、winscp，数据库：ssms、sqlwb、mysqlworkbench、mysql、dbvisualizer、plsql、sqlplus、toad、db2cmd、quest central、navicat，无需应用发布服务器（提供产品功能截图） |
| URL访问管控 | 支持对HTTP/HTTPS类资产进行URL黑白名单限制，禁止在未授权情况下，通过手动输入URL跳转至其它web网站。 |
| 数据库兼容性 | ★标准支持DB2、oracle、mysql、sqlserver、PG、人大金仓、达梦数据库的协议运维代理，可实现自动登录，自动登录可直接调用本地windows系统的数据库客户端工具（包括ssms、sqlwb、workbench、mysql、DbVisualizer、plsql、sqlplus、toad、dbcmd、Quest Central、pgadmin3、psql、ksql、Isql、DIsql、DMmanger、navicat等），无需应用发布前置机（提供产品功能截图） |
| MAC兼容性 | ★支持在Mac操作系统下调用navicat工具运维mysql、oracle等数据库资产（提供产品功能截图） |
| 数据库命令管控 | 数据库支持命令阻断功能，精确到数据库，表、字段级别（提供产品功能截图） |
| 数据库双重审计 | ★支持同时对数据库会话记录图形审计及命令提取；支持对数据库运维会话的上行和下行命令进行审计。（提供产品功能截图） |
| 运维管理 | 支持B/S架构进行堡垒机运维管理，至少支持使用IE、谷歌、火狐、Microsoft Edge等浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等本地运维客户端工具 |
| 专用客户端运维 | ★支持Windows/macOS操作系统下C/S架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作。（提供产品功能截图） |
| SSH网关代理直连 | ★支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备。（提供产品功能截图） |
| SSH-agent-forwarding | 可以使用SSH-agent-forwarding登录到SSH服务器，用于登录堡垒机和登录SSH主机使用相同私钥的场景。 |
| 禁审功能 | ★支持提供禁止审计功能，可对部分设定策略的会话不审计录像，防止机密信息二次泄漏。（提供产品功能截图） |
| 运维会话自审 | 支持运维用户查询用户本人的运维审计会话，减轻审计管理员的负担，并且帮助运维用户提高运维效率 |
| 实时监控 | 支持对文件传输会话的实时监控。 |
| 文件传输管控 | 支持对SFTP、FTP、ZMODEM进行文件传输控制，支持禁止文件上传、下载、删除、重命名，支持禁止对目录的创建与删除；支持对RDP会话的剪贴板、磁盘映射的文件传输控制。 |
| 运维规则策略 | 支持通过基于时间、IP/IP段、用户/用户组、主机组、主机账号、命令控制策略等组合访问控制策略，授权用户可访问的目标设备。 |
| 命令审批 | 支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令。 |
| 国密TLS单向通信 | ★支持国密TLS单向认证通信，使用国密算法保证HTTPS协议层面的数据机密性和完整性；开启后需使用支持国密算法的浏览器才能访问堡垒机（提供产品功能截图） |
| 配置备份 | 系统配置文件支持自动备份到FTP/SFTP服务器上，支持配置备份周期。 |
| 存储管理 | 支持NAS/CIFS存储（提供产品功能截图） |
| API接口 | ★需提供用户、资产、授权的增删改查等API接口，允许第三方平台调用堡垒机的API接口，实现用户、资产、权限自动同步到堡垒机，简化堡垒机配置工作量。（提供产品功能截图） |
| 跨地域部署 | 支持多台堡垒机异地备份部署，每台设备都能提供运维和审计服务，配置数据自动同步。 |
| 资质要求 | 具备计算机信息系统安全专用销售许可证证书具备国家信息安全 信息技术产品安全测评证书（EAL3+） |

## 2、VPN设备增加授权

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 性能要求 | 原天融信VPN设备增加100个ssl vpn授权 |

**三、商务需求**

1. 〈一〉中标产品应完全满足技术规格要求，不满足作废标处理。

〈二〉中标人应免费将所供产品运输到用户指定地点，用户组织产品供货验收合格后，根据用户要求免费实施产品的安装调试。

〈三〉本次采购产品，需要对接医院的各项信息平台，需要把资产加入堡垒机中。

2、付款方式：所有设备到货安装调试完毕，经用户核对验收后，支付100%；

3、〈一〉安装地点：用户指定施工地点。

〈二〉完成时间: 合同生效后20个工作日内必须将所有设备调试安装完毕。

〈三〉安装标准：符合我国国家有关技术规范要求和技术标准，所有的设备必须保证同时安装到位。

〈四〉中标人免费提供中标设备的安装服务。

〈五〉调试所需专用工具设施材料由中标方自备、自运到现场，完工后自费搬走。

4、保修及服务：〈一〉提供原厂三年保修，保质期内因设备本身缺陷造成各种故障应由卖方免费技术服务和维修。

〈二〉在质保期内，所有因服务、设备及零部件更换和维修等原因产生的费用由供应商承担。同时,在整个产品使用期内中标人应确保产品的正常使用，在接到用户维修要求后应立即作出回应，当系统的软硬件设备出现故障时，供应商也应承诺在接到买方通知后30分钟内响应并提出解决方案，在1小时以内完成甲方提出的维修要求，如需更换设备或送修，必须在2个工作日内负责解决。如无法解决问题，应提供同档次的设备予以代用。