中国医学科学院肿瘤医院

堡垒主机

技术需求

**信息中心/计算机室**

**2017年8月**

堡垒主机技术需求

1. **项目说明**

《信息安全等级保护基本要求》中，针对主机安全、网络设备防护、安全审计作出规定。要通过三级等保测评，需要增加堡垒主机来实现这些功能要求，

1. **采购数量：1台**
2. **技术参数要求**

|  |  |  |
| --- | --- | --- |
| 硬件参数 | 基本要求 | 2U机架式软硬一体设备，支持4个千兆电口，可扩展至2\4光（SFP），内存4G，硬盘2T。 |
| 性能要求 | 并发会话数：字符不低于1500个，图形不低于300个 |
| 高可用性 | 双机热备 | 支持主/备模式双机热备部署，业务数据实时同步，主/备机切换时间不大于3秒。 |
| 网卡冗余 | 支持双网卡冗余配置 |
| 配置要求 |  | 授权数不少于200，与LanSecS-NK-200实现双机热备 |
| 安全要求 | 会话安全 | 提供认证服务器组件，所有对资源从账号的访问都是认证服务器提供的临时会话号，即使该会话号被截获，也无法通过此会话号再次访问资源，从而提高资源访问的安全性。运维人员通过WEB登录内控管理平台访问授权资源时，看不到被管资源的帐号/口令，只能开到一次性会话号。会话号按照票据(token)认证规范进行开发 |
| 扩展要求 | 第三方CA认证 | 提供对第三方CA认证服务的认证支持，至少支持北京CA、上海CA、吉大正元、上海格尔、总参56所等厂商 |
| 业务数据存储 | 业务数据采取轻型目录存储（LDAP），支持多台内控管理平台间的业务数据实时同步 |
| 支持协议 | 字符协议 | TELNET、SSH1、SSH2 |
| 图形协议 | RDP、VNC、X11 |
| 文件传输协议 | FTP、SFTP、windows文件共享 |
| 数据库 | 支持ORACLE、MSSQL、Sybase、Mysql、DB2数据库远程访问协议审计 |
| B/S、C/S应用扩展 | 支持通过外置应用发布进行协议扩展，支持B/S应用系统的应用发布。支持定制开发其他访问协议及第三方客户端工具 |
| 支持主机 | 主机 | Windows类主机、Unix类主机、Linux类主机 |
| 网络设备 | 网络设备（思科、华为、H3C、中兴、锐捷等） |
| 防火墙/安全设备 | 支持各类B/S架构防火墙及安全设备 |
| 产品功能 | 身份认证与访问授权 | 支持多种认证方式：静态口令认证、RADIUS认证、动态口令认证、LDAP认证、AD域认证、CA证书认证、第三方指纹认证、人脸识别等  支持上述双因素或多因素组合认证方式 |
| 支持自主发放软/硬证书，不依赖第三方PKI体系 |
| 支持运维管理三员，三员之间相互独立相互制约 |
| 单点登录 | 提供统一登录页面，作为用户登录各系统资源的统一入口，集中控制用户能够访问的系统资源以及B/S、C/S应用资源，统一提供HTTPS访问的B/S登录页面并提供资源从账号访问链接，用户点击相应资源从账号链接后直接登录到目标资源，整登录个过程对用户透明。 |
| 支持双人共管账号的单点登录及主副岗管理从账号的单点登录 |
| 支持常用单点登录工具，支持SecureCRT、xshell、NetTerm、SSH Secure Shell、Mstsc等系统原有客户端登陆进行操作，同时支持特殊运维工具的定制扩展。SSH、telnet协议代理支持客户端软件的Session Clone及Send To All等复杂的功能。 |
| 访问控制 | 支持对违规或高危操作的指令进行阻断或审批处理；支持指令黑白名单。 |
| 支持对违规或高危指令的正则匹配 |
| 支持基于登录时间、登录IP地址、登录客户端MAC地址的强访问控制 |
| 支持以FTP策略的形式对FTP/SFTP、windows文件共享的传输进行限制 |
| 支持用户多次登录失败自动锁定功能，支持系统自动解锁和管理员手动解锁功能 |
| 用户及组管理 | 支持主账号的全生命周期管理，包括添加、修改、删除、锁定、解锁、注销功能 |
| 提供可多级扩展的的组管理模式，在相应组下可建立主账号或资源、资源从账号，审计查看、管理权限划分可依据树形组作为范围区分。 |
| 支持运维用户组的管理，包括添加、修改、删除、移入、移出组成员功能 |
| 可以根据工作的需要，将用户按照多角色划分，至少可以划分为管理员、审计管理员操作运维用户三种角色，其中管理员和审计员均可依据树形组限定范围区分管理范畴。 |
| 支持从LDAP目录（如windowsAD域）中抽取用户作为系统的主账号 |
| 主机及组管理 | 支持主机管理，包括主机IP、主机名称、主机类型、访问协议及端口、主机帐号及密码等信息 |
| 支持组管理模式，主机资源可分配给不同的管理组 |
| 密码托管 | 支持运维用户、目标设备口令的密码强度进行管理 |
| 支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。 |
| 支持密码策略设置，可自定义密码复杂程度，可设置密码中包含数字、字母、符号及禁用关键字等内容 |
| 支持密码文件备份功能，密码文件需密文保存，下载后需解密处理 |
| 支持密码信封打印机功能，可打印纸质密码信封，留存纸质存档 |
| 操作审计 | 支持对字符协议、图形协议、数据库操作、应用发布内容进行屏幕录像审计 |
| 支持全程记录图形协议操作内容 |
| 支持记录字符型运维协议的操作命令和屏幕回显 |
| 管理行为审计：系统除提供行为审计外，也需提供内部操作审计。审计内容需包括运维“三员”登入、登出、配置管理、策略修改、用户属性修改等操作。 |
| 支持高级检索询功能，用户可按用户账号、资源账号、资源IP、起止时刻、资源类型、协议类型、会话关键字等字段组合查询审计记录。 |
| 支持审计日志防溢出功能，存储空间不足时能够选择清理老旧数据 |
| 支持日志文件的外挂存储配置 |
| 操作回放 | 支持以WEB在线视频回放方式重现维护人员对服务器的所有操作过程，无须在客户端安装播放客户端软件 |
| 录像画面清晰流畅，支持不同色彩，支持多种不同分辨率。 |
| 支持播放速度调节、拖动、暂停等播放控制操作 |
| 支持从指定指令进行定位回放 |
| 支持下载录像文件到本地加密保存，只能通过专用播放器查看，防止会话视频记录泄密 |
| 操作监控 | 支持对回话进行实时监控、回放和阻断操作 |
| 支持实时监控堡垒主机CPU、内存、磁盘的使用情况 |
| 操作报表 | 支持按用户、时间、主机类型等字段生成审计报表 |
| 支持以Word、Excel和pdf方式生成并导出报表 |
| 支持管理员自定义审计报表,支持图形报表。 |
| 登录审批流程 | 对目标设备的访问支持审批流程。普通用户访问特定目标设备时，需发起访问申请至指定审批人，审核通过后才能对特定目标设备进行访问。 |
| 产品应包含事前审计功能，可强制用户在申请访问时填写申请原因。 |
| 支持对任意目标设备上的账号指定审批人及审批类型（审批类型至少包括：单人审批授权、双人授权审批）。 |
| 申请及审批具有时效性，并且可自定义有效时限。 |
| 申请、审批等未完成操作可通过邮件进行通知提醒。 |
| 产品应支持对未能通过审批的申请禁止被使用。 |
| 产品应支持对通过审批，但超过有效期限的申请，应禁止访问目标设备或系统自动注销超出时限的运维回话，为保障运维过程连续性，即将达到申请有效期前应当给予操作人提示，并提供仅允许一次的延时选项，方便运维人员主动保存工作进度。 |
| 产品应支持申请及审批流程的集中归档记录。 |
| 审批人不能查看特权帐户的权限。 |
| 批操作 | 支持通过手动或Excel表格导入的方式批量添加主、从账号 |
| 支持通过手动或Excel表格导入的方式批量添加被管理员资源 |
| 支持批量账号授权 |
| 系统管理 | 支持NTP系统时间同步配置，保证审计日志拥有可靠的时间戳 |
| 支持告警对外转发，转发方式支持syslog、snmp trap、邮件等方式 |
| 支持堡垒主机端口配置，可配置关闭不必要的端口 |
| 资质要求 | 产品资质 | 产品具有公安部颁发的《计算机信息系统安全专用产品销售许可证》， 并提供证书复印件 |
| 产品具有国家版权局颁发的《计算机软件著作权登记证书》，并提供证书复印件； |
| 产品具有国家保密局颁发的《涉密信息系统产品检测证书》 |
| 产品具有中国信息安全认证中心颁发的《IT产品信息安全认证证书》 |
| 产品具有国家信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL2级或以上） |
| 项目经验 | 投标方经验 | 具有同类产品大型项目承建经验（产品采购数量在30台以上） |

1. **服务要求**

提供三年原厂免费服务，包括软件升级，硬件质保，现场技术支持服务，永久电话支持服务。