堡垒机1台

|  |  |  |
| --- | --- | --- |
| 指标名称 | 指标项 | 详细描述 |
| 资质要求 | 产品资质 | 计算机软件著作权登记证书；国家公安部计算机信息系统安全专用产品销售许可证；IT产品信息安全认证证书国家涉密信息系统产品检测证书；IPV6Ready认证证书；产品必须是自主研发而不是OEM产品； |
| 生产商资质 | 拥有省级以上高新技术企业资质；通过ISO9001:2015质量管理体系认证； |
| 系统架构 | 产品架构 | 软硬件一体化产品，采用标准机架式硬件结构； |
| 操作系统 | 深度定制优化的Linux系统； |
| 部署方式 | 旁路代理模式，不影响正常业务流量； |
| 高可用性 | 支持双机热备部署； |
| 集群部署 | 支持集群化部署 |
| 管理结构 | B/S架构，采用HTTPS方式远程安全管理，无需安装管理客户端； |
| 应用发布 | 支持内置、外置应用发布同时使用； |
| 性能要求 | 网络接口 | >=100/1000M RJ45\*4个自适应以太网口； |
| 存储性能 | 内存>=16G，存储空间不低于2TB； |
| 可管理对象数量 | 内置200个主机/设备操作监控许可证书； |
| 并发会话数 | 图形并发会话数>=300字符型并发会话数>=700 |
| 系统先进性 | 产品先进技术  | 提供安全终端仿真协议监控时实现会话复制和跟踪的方法的技术先进性证明；（提供相关证明材料）提供FTP二次登录系统及实现文件传输和过程监控方法的技术先进性证明；（提供相关证明材料）提供实现远程虚拟桌面访问统一管理和监控的系统及方法的技术先进性证明；（提供相关证明材料）提供在远程桌面传输协议监控时实现操作识别的系统及方法的技术先进性证明；（提供相关证明材料） |
| 功能要求 | 支持协议 | 字符型远程操作协议：SSH(V1、V2)、TELNET、RLOGIN、AS400；图形化远程操作协议：RDP、VNC、X11；文件传输协议：FTP、SFTP； 数据库远程操作协议：支持ORACLE、MSSQL、Sybase、Mysql、DB2数据库远程访问协议审计；支持通过应用发布的代理进行协议扩展，支持Radmin、Pcanywhere、 HTTP/HTTPS，可自定义其它访问协议及客户端支持；支持应用发布方式HTTP越权访问提示及阻断功能；支持协议端口自定义； |
| 主机运维及访问方式 | Web方式访问支持所有远程协议；支持HTML5调用，运维操作无需JAVA支持和客户端；支持MacOS调用SecureCRT进行运维；支持国产化桌面操作系统调用本地客户端进行运维；Web访问方式支持IE、Edge、Firefox、Chrome、Safari等所有主流浏览器；通过的Web页面直接访问服务器或通过WEB页面调用本地工具（含数据库官方客户端）直接访问服务器；web访问方式支持历史访问配置参数自动记忆功能；通过web调用客户端方式使用SSH协议支持会话复制功能及支持直接调用SFTP功能；使用RDP协议支持剪切板、磁盘映射功能；支持在web页面上进行连接测试（PING、TRACEROUTE、TELNET）； |
| 客户端访问方式：支持通过管理员常用的客户端(如SecureCRT、PUTTY、Mstsc、PLsql、SQLplus等)直接连接堡垒机再访问到服务器；支持客户端(如SecureCRT、putty)会话复制功能；支持SSH软件中直接调用sftp功能； |
| 资源菜单访问方式：客户端访问审计系统即可显示用户能访问的主机资源菜单，用户通过字符菜单或图形菜单选择列表方式直接访问服务器； |
| 菜单方式访问支持所有协议；支持双人协同操作功能；支持会话批量连接登录功能；支持批量执行并对批量执行结果进行成功或失败判断； |
| 身份认证 | 支持多种认证方式：本地密码认证、UsbKey认证、TOTP令牌认证、第三方CA证书认证、指纹认证、google身份验证APP验证、邮件认证、RADIUS认证、LDAP认证、AD域认证以及短信认证；支持邮件/短信方式密码自助找回功能；支持登录输错2次自动开启验证码功能；支持企业微信发送登录验证码功能（提供相关Web页面截图和企业微信截图证明）；可使用厂商提供的小程序完成TOTP认证，不需要安装app；（提供微信小程序截图证明）支持采用oauth2协议与IAM系统进行对接，完成身份验证和授权；（提供IAM配置截图、堡垒机页面截图、IAM代码片段截图和堡垒机代码片段截图证明） |
| 访问授权 | 支持SSO功能，运维人员不必输入服务器帐号及密码，无需进行二次登录认证；支持通过基于时间、IP/IP段、用户/用户组、设备/设备组、设备账号、命令关键字、命令关键字、黑白名单等组合访问控制策略，授权用户可访问的目标设备。支持粗放式访问授权模式，授权条件仅基于运维用户（用户组）和目标主机IP地址段，不限制使用的系统账号及协议等其它条件；支持审批模式：运维用户访问特定的服务器设备必须经过管理员的临时审批授权才能进行，否则无法进行任何操作；（提供相关Web页面截图证明）支持对重要设备启用登录审核策略：运维人员须向管理员申请登录，管理员允许之后才可登录，否则无法登录支持对重要设备启用登录备注策略：运维用户访问设备时必须先填写该次访问的目的等内容，否则无法登录；支持对重要命令进行实时审核：运维人员执行命令后，系统响应动作包括：指令审批、忽略指令、阻断会话、产生告警；（提供相关Web页面截图证明）支持工单授权功能：通过运维人员申请或管理员下发工单的方式来赋予运维人员访问目标服务器的权限，且有工单生效时间限制；（提供相关Web页面截图证明）支持登录预处理命令设置；（提供相关Web页面截图证明）支持设定会话连接单位时间内空闲无操作，连接自动断开；（提供相关Web页面截图证明）支持登录预处理命令设置：登录成功后，自动执行指定的操作命令（提供相关Web页面截图证明）支持所有访问授权策略导出及是否覆盖性导入功能（提供相关Web页面截图证明）支持权限拓扑功能，可根据用户名或主机查看对应权限及相关用户或主机；（提供相关Web页面截图证明） |
| 访问控制及异常告警 | 支持运维用户多次登录失败自动锁定账号功能及解锁机制设定；支持审计限制策略：限定管理员针对指定的运维用户的运维记录进行审计；支持授权限制策略：限定管理员针对指定的运维用户进行授权管理；支持按用户（用户组）、目标设备（设备组）、系统帐号、命令集和生效时间等内容或按访问授权策略设定安全事件规则；支持运维用户多次登录失败自动锁定账号功能及解锁机制设定；支持异常登录告警功能；RDP剪切板支持单向传输控制；支持FTP/SFTP上传下载控制；支持IP地址/MAC地址限制功能；支持协同会话功能；支持运维空闲会话时间全局设置限制功能支持以屏幕、邮件、SYSLOG、Snmp Trap、短信方式实时发送告警信息；支持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、移动MAS联动（提供相关Web页面截图证明） |
| 用户管理功能 | 支持添加、删除、修改以及启用、停用运维用户；支持用户多角色划分功能，如系统管理员、配置管理员、审计管理员、密码管理员、审计审计员、运维用户等，对各类角色可组合进行细粒度的权限管理每个部门的部门管理员可以管理本部门及下级部门的主机、授权关系、策略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、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录IP范围等；支持AD域用户、LDAP用户按组织架构批量导入。支持用户/用户组的多级架构管理，可以复制、剪切、粘贴、移除用户/用户组，实现用户/用户组架构的灵活调整；（提供相关Web页面截图证明）支持用户授权快速绑定及集成、移交功能，可以将用户的群组属性和权限交接给其它用户（提供相关Web页面截图证明）支持多种认证方式：本地静态密码认证、原厂商UsbKey认证、原厂商动态令牌认证、第三方CA证书认证、指纹认证、TOTP认证、RADIUS认证、LDAP认证、AD域认证以及短信认证；（提供相关Web页面截图证明）支持认证方式全局设定、单一用户认证方式设定，支持多种认证方式组合；（提供相关Web页面截图证明）支持运维账号使用有效期管理；支持运维用户密码强度管理；用户帐号支持管理员和运维人员双重身份； |
| 主机管理功能 | 支持主机/主机组的多级架构管理，可以复制、剪切、粘贴、移除主机/主机组，实现主机/主机组架构的灵活调整（提供相关Web页面截图证明）支持系统类型管理：内置常见系统类型，可自定义添加目标设备的系统类型及内容，包括显示图标、该系统拥有的协议及默认端口等内容；支持添加主机页面在线ping主机功能，即时获取该主机存活信息；支持在添加主机页面对主机账号及协议通道验证功能，即时获知该账号及访问通道是否有效，并设定周期性自动验证；（提供相关Web页面截图证明）支持常用的运维协议：SSH、TELNET、RDP、FTP、SFTP、Oracle、Mysql、Sybase、DB2、MSSQL（提供相关Web页面截图证明）支持oracle、mysql主流数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机（提供相关Web页面截图证明）支持系统类型管理：内置常见系统类型，可自定义添加目标设备的系统类型及内容，包括显示图标、该系统拥有的协议及默认端口等内容；支持在线ping主机功能，即时获取该主机存活信息；支持批量导入主机，且在批量导入中自动进行连接测试；（提供相关Web页面截图证明）支持主机登录限制，同一台服务器可以只允许一个用户登录，防止已登录用户被登出；（提供相关Web页面截图证明）支持自动发现主机，可设定检测网段和服务端口进行扫描；支持IP地址集、时间集、指令集管理功能；主机SSH运维支持密钥托管功能； |
| 操作行为记录 | 支持对运维操作会话的在线监控、实时阻断、会话回放、起止时间、来源用户、来源IP、目标设备、协议、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。支持对RDP标题窗口、键盘输入的记录和搜索定位（提供相关产品截图证明）支持全字段搜索审计日志，只需通过关键信息快速搜索定位支持将常用查询条件设定成模板，供多次引用（提供相关产品截图证明）支持查询结果加密导出支持日志关联分析，可直接关联到日志同个会话中的所有操作日志（提供相关产品截图证明）支持会话录像在线回放、定位回放及下载后使用官方专用客户端离线回放（提供相关产品截图证明）支持审计数据按时间区间进行备份，按周期及磁盘配额进行自动归档，并通过FTP方式自动上传保存 |
| 会话过程回放 | 支持倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作；支持从特定操作指令开始进行定位回放；（提供相关产品截图证明）；支持MacOS播放下载到本地的视频；（提供相关产品截图证明）支持回放界面中显示键盘输入、功能键、鼠标动作；支持下载回放文件到本地保存，并通过厂家专用播放器查看，防止会话视频记录泄密；（提供相关产品截图证明） |
| 密码管理 | 改密类型支持Windows、Linux、Unix、AIX、Cisco、HUAWEI、H3C、Ruijie等；（提供相关产品截图证明）支持按设备、数据库、系统帐号、计划执行时间、改密周期、密码策略、改密结果发送等生成详细的改密计划，到期自动执行；支持使用agent方式修改主机密码；（提供相关产品截图证明）支持随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并能严格遵守密码强度设置；（提供相关产品截图证明）支持手工执行改密功能；支持改密结果自动发送至密码管理员或FTP上传；支持手工下载全部或部分主机密码功能；支持自动改密结果报表；支持密码金库模式导出，即多个管理员拥有密码的不同分段提供相关产品截图证明）支持改密多人审批； |
| 实时监控 | 支持实时监控近期发生的所有会话信息，显示会话状态（连接中、退出、阻断）；支持对会话进行同步监控，执行会话回放、监控和阻断操作；支持实时监控审计系统CPU、内存、磁盘的使用情况；支持记录审计系统自身的管理操作，保障审计系统自身安全； |
| 历史查询及审计报表 | 支持单一条件快速查询、查询结果二次过滤以及多重条件组合高级查询功能；（提供相关产品截图证明）支持同一次会话中的指令关联查询，显示会话中所有操作指令；支持根据查询结果直接定位视频文件，回放历史会话；内置丰富的报表统计模板，且支持PDF、doc、html、RTF、XLS、ODT格式导出；支持自定义报表模板：支持用户配置报表生成条件及报表内容，可生成统计型、明细型报表，图形报表、文字报表；（提供相关产品截图证明）支持以日报、周报、月报的方式自动生成周期性报表，并自动发送至指定邮箱； |
| 数据安全管理 | 提供专用数据存储系统的著作权证书；提供高性能日志及行为审计系统证书；支持国产加密算法对数据进行加密；（提供相关产品截图证明）支持采用国产加密算法证书对http通信对进行加密；（提供相关产品截图证明）提供国产加密算法改造方案说明和完成国产加密算法改造用户的感谢信以证明产品可以帮助用户通过国产加密算法测评。（提供国产加密算法改造方案和用户感谢信证明）支持自动归档和手动备份、支持以FTP方式自动上传归档数据；支持备份数据恢复导入；支持空间自管理功能，存储空间不足时能够自动清理老的数据；支持系统配置的导入、导出功能； |
| 协同操作 | 支持双人协同操作功能；（提供相关产品截图证明） |
| 批量执行 | 支持批量执行功能；（提供相关产品截图证明）支持会话批量连接登录功能；（提供相关产品截图证明）支持对批量执行结果进行成功或失败判断；  |
| 消息中心功能 | 支持工作任务流程及消息中心管理功能：支持用户间互相发送消息，通过消息下发工作任务等功能；（提供相关产品截图证明）支持关键事件自动生成消息如：二次审批、备注审批、协同操作邀请； |
| 系统管理功能 | 支持页面证书下载；支持生成自签名的RSA算法的SSL证书和自签名的国产加密算法的SSL证书；（提供相关产品截图证明）支持RSA算法的SSL证书和国产加密算法的SSL证书上传；（提供相关产品截图证明）支持页面下载系统相关软件；支持系统时钟手工配置，支持NTP时间同步配置；支持系统配置文件导入及导出功能；支持从WEB界面修改网卡IP设置、静态路由设置等内容；支持从Web界面配置BOND；支持修改不同访问模式（客户端直连、菜单方式）的默认访问端口支持从WEB管理界面重启、关闭设备；支持页面超时设置；支持通过web界面进行系统升级；支持系统运行日志、系统操作日志的查询和统计；提供在线排错工具：ping、telnet、tracerroute支持自定义运维协议代理端口号、支持启停运维协议服务支持系统硬件、系统服务进程、数据库、应用代理进程状态实时在线监控支持页面管理硬盘并进行更换（提供相关产品截图证明）；支持邮件、短信、Syslog、FTP、SNMP等输出接口配置支持系统告警日志发送； |
| 其他要求 | 产品授权及服务 | 提供针对本项目的原厂授权函；提供原厂三年7\*24小时的售后服务承诺；提供三年原厂保修及原厂免费现场服务，产品的安装、培训由原厂工程师完成实施；在设备维保期内，厂家提供对系统软件的免费升级服务，保证系统软件为最新版本。 |

上网行为管理1台

|  |  |
| --- | --- |
| **功能项** | **功能要求说明** |
| ▲规格要求 | 网络层吞吐量≥10Gb，应用层吞吐量≥1.5Gb，带宽性能≥1Gb，IPSEC VPN加密性能（最高性能）≥200M，包转发率≥130Kpps，每秒新建连接数≥14000，最大并发连接数≥600000，支持用户数≥1500，接口:6千兆电口；2千兆光口SFP。 |
| 多主模式 | 支持两台及两台以上设备同时做主机的部署模式；  |
| VPN组网 | 支持IPSec VPN模块，支持与LDAP服务器、Radius服务器、硬件特征码绑定认证；VPN支持多线路，通过配置主备线路组和流量分配模式的多线路选路策略； |
| 实时状态 | ★支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；（提供产品界面截图） |
| 故障排查 | 支持网络故障排查，支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况； |
| 用户认证故障排查，支持针对用户认证的故障进行分析，给出错误详情以及排查建议； |
| ★SSL解密故障排查，支持客户端解密排障，自动检测解密审计不成功原因；（提供产品界面截图） |
| Web访问质量检测，针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级； |
| 密码安全 | 可设置密码最小长度、复杂度，可设置密码不能与用户名相同、新密码不能与旧密码相同 |
| 特权DKey | ★支持针对特权用户配置免认证key、免审计key、免控制key；（提供产品界面截图） |
| 本地认证 | 支持用户名密码认证、IP/MAC认证、短信认证等本地认证方式 |
| 协同办公认证 | 支持通过钉钉、企业微信、口袋助理等第三方协同办公软件进行授权认证； |
| 短信和微信快捷认证 | 支持终端用户账号绑定手机号码和微信号，绑定后可以通过手机验证码和微信扫码实现上网快捷登录认证； |
| 双因素认证 | 支持账号密码+动态令牌（Authenticator APP）验证码身份认证，支持通过短信和密码绑定动态令牌； |
| P2P智能流控 | ★支持通过抑制P2P的下行丢包，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；（提供产品界面截图） |
| 应用识别规则库 | 设备内置应用识别规则库，支持超过9000种以上应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制； |
| SaaS应用规则 | 支持超过900种主流Saas应用，对Saas应用有默认分类标签，帮助客户统一配置策略；（提供产品界面截图） |
| URL库管理 | 能够针对各种URL类型做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制； |
| 内置URL数量在3000万以上，包含分类数量150个以上；管理员可自定义新的URL地址和URL分类； |
| 网页访问审计 | 支持记录全部或者指定类别URL、网页标题、网页内容等信息，支持网页内容审计后的网页快照功能； |
| 加密网页管理 | ★支持SSL加密网页的内容检查，可对SSL加密网页进行解密并识别、过滤其内容，针对加密后的钓鱼网站、非法网站，可对用户进行重定向告警；（需提供第三方检测报告或自主知识产权证明） |
| ★支持客户端SSL解密，客户端会自动推送根证书安装；（提供产品界面截图） |
| 审计SSL网页时，支持加密证书重定向分发功能； |
| Webmail管理 | 支持允许用户登录Webmail收邮件，而禁止发送Webmail邮件的功能；（提供产品界面截图） |
| 加密邮件识别 | 支持对加密HTTPS、SMTP-SSL、SMTP的邮件进行识别； |
| 防共享接入 | 支持发现私接路由（或者共享软件等）共享网络的行为，支持“仅统计电脑”和“统计所有终端”两种模式，自定义配置终端数量和冻结时间，支持添加信任列表，支持例外排除功能；能针对行识别校园网破解版路由器 |
| IP地址管理 | 支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量；（提供产品界面截图） |
| 终端资产识别 | 自动发现网络里面的终端，并获取IP、Mac、厂商、操作系统等信息，设备必须支持PC、移动设备、哑终端、专用设备的发现和型号识别：至少支持Windows、Linux、MAC、瘦客户机等PC；至少支持手机、平板等移动设备；至少支持服务器、交换机、无线控制器等网络设备；至少支持打印机、投影仪、电视、摄像头、门禁系统等哑终端；支持自定义终端类型； |
| 业务系统自定义 | 支持自定义业务系统名称、描述，绑定到相应的IP地址和端口或域名，以每个业务系统作为单独审计对象； |
| 业务访问审计 | 支持WEB/FTP/SMB类型业务的行为和内容审计，对上传/下载文件可选择只审计文件名或同时审计文件内容； |
| 安全态势感知产品联动 | ★支持与客户侧现有的安全态势感知产品实现联动，实现同步用户认证信息、弹窗提醒和冻结账号的功能、实现资产信息上报;（提供产品界面截图） |
| 投标产品资质要求 | 具备中国信息安全测评中心颁发的《国家信息安全测评/ 信息技术产品安全测评证书（级别：EAL3+）》，需提供有效证书复印件。 |
| 所投产品应具备相当的技术认可度，产品曾连续两年入围Gartner SWG魔力象限，需提供有效证明材料 |
| 投标产品生产商资质要求 | 所投厂商应具备国家互联网应急中心 CNCERT网络安全应急服务支撑单位（国家级），需提供相关证明材料。 |
| 所投厂商应是国家标准《信息安全技术网络安全审计产品技术规范》主要起草单位，需提供相关证明材料。 |