国家税务总局珠海市税务局

运维安全审计设备(堡垒机)采购在线询价文件

国家税务总局珠海市税务局

2021年9月

一.技术规格、参数与要求

1.1设备采购清单

本次项目所需采购的设备清单如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **规格描述** | **数量** |
| 1 | 运维安全审计设备 | 详见具体技术参数指标 | 1台 |

1.2 技术参数指标

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| **★硬件要求** | 2U机型，提供1个console口，2个USB口； ≥6个千兆电口，≥4个SFP插槽，不少于2个可扩展插槽，双电源。 |
| **★性能要求** | 提供200个资源授权，用户数不限制；支持资源授权后续可扩展总数2000个 |
| **基本要求** | 专用的硬件和软件保障 | 采用专用硬件架构与安全操作系统，硬件设备可以机架安装。 |
| 硬件模块化设计 | 产品采用模块化设计，可以通过扩展卡来增减业务接口，而非软件运维安全审计系统 |
| 采用多核CPU | 采用多核多线程CPU处理器 |
| **部署方式** | 工作模式/高可用 | 采用物理旁路部署，不改变现有网络结构；支持双机部署，保证系统发生故障时的可用性；支持自建集群部署：支持无缝横向扩展，轻松应对高并发需求； |
| **用户管理** | 用户管理 | 支持用户的增删改查、锁定、激活，进行用户全生命周期管理，支持用户批量导入和导出；支持用户清理功能 |
| 角色管理 | 支持系统管理员、保密管理员、密码管理员、安全审计员、保密员、运维管理员、操作员七种角色，同时也可按需分配角色权限，权限间相互制约； |
| 认证管理 | 支持本地认证和三方认证服务器接入认证，如AD、LDAP、Radius服务器； |
| 支持密码认证、证书认证、USBKEY认证、人脸识别等双因素认证方式； |
| 证书管理 | ▲支持第三方证书用户自行上传用作校验的CA证书和CRL列表；本地CA支持根证书的重新生成及替换；支持根据根证书签发出客户端证书；支持发布生成吊销列表；支持国密证书认证。（提供界面截图并加盖原厂公章） |
| 用户分组 | 归属层级化部门分组管理；用户组与部门关联，支持部门隔离；支持授权和规则配置用户组； |
| 消息管理（公告） | ▲支持管理员通过发布公告的形式，发送通知给所有指定用户； （提供界面截图并加盖原厂公章） |
| 认证服务器同步 | 支持通过AD域服务器和LDAP服务器进行用户同步； |
| **资产管理** | 资产管理 | ▲支持混合云资源的管理，即公有云及局域网资源，支持主机、服务器、网络设备、安全设备、数据库等的资产管理；（提供界面截图并加盖原厂公章）满足公有云、云资源池、数据中心多种运维场景； |
| ▲支持首页动态展现资源总量、活动用户、实时会话、待审批工单、当日运维记录、资产运行状态、今日运维总数、今日运维时长TOP10、今日告警总数、今日运维指令TOP10等信息，方便管理员实时查看系统运行情况掌握资产会话连接情况。（提供界面截图并加盖原厂公章） |
| 支持资源分类和资源系统类型管理：内置常见资源分类和资源系统类型，可自定义添加资源分类、资源系统类型和资源服务类型； |
| 自动发现 | ▲公有云设备支持一键更新发现功能；支持自动扫描网段内主机并支持导入系统（提供界面截图并加盖原厂公章） |
| 云同步 | 支持华为云、阿里云、腾讯云主机同步功能； |
| 资产组管理 | 支持资产组的增删改查； |
| 资源导入导出 | 支持资源（包括服务和资源账号）批量导入导出功能； |
| 批量运维 | 支持创建不同资产，不同协议的批量运维登录 |
| 特权切换 | 支持以普通管理模式登录网络设备或主机并自动切换到特权模式。 |
| Session导出 | 支持Xshell、Xftp、SecureCRT客户端的session文件导出 |
| **账号管理** | 密码托管 | 支持对已添加的设备账号进行密码托管，从而实现单点登录功能； |
| 账号改密 | 自动对数据库、Windows、Linux等设备进行账号改密，改密支持手动和定期任务，密码配置支持全局策略和手工指定，密码复杂度支持按策略随机生成； |
| ▲支持改密结果自动发送到制定改密计划的管理员邮箱；密码采用密码信封加密保存，以保证安全性；支持密码分段发送。（提供界面截图并加盖原厂公章） |
| 批量操作 | 支持账号批量修改、删除等操作； |
| 登录方式 | 支持自动、半自动、手动三种登录方式； |
| **权限管理** | 授权管理 | 支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权； |
| 运维策略 | 支持会话、指令、剪切板上下行、文件上传下载的约束行为； |
| 登录策略 | 支持对用户/IP/mac地址/登录时间进行控制； |
| 运维工单 | 支持内置工单运维，操作员可根据工作需求临时申请设备运维工单，管理员审批后可直接运维，过期失效； |
| 授权关系 | 提供授权关系查看功能，图形化直观展示用户、资产、协议、账号的授权关系；  |
| 访问策略 | 支持对运维时间、运维地址、运维操作指令、操作行为的限定，触发策略后进行告警、再审、阻断等； |
| 组管理 | 支持地址、时间、指令单独组配置，进行批量管理； |
| **设备访问** | 单点登录 | 支持访问SSH、RDP、Telnet、FTP、SFTP、VNC、数据库等资产；支持无须记忆多个设备账号和密码，实现账号密码代填功能；支持自动、半自动、手动三种登录方式；支持进行协议/工具扩展； |
| Html5技术 | ▲设备访问支持最新的html5技术，在同一WEB窗口页签中，无需JAVA应用插件或调用本地应用客户端，即可实现对目标设备的快速运维；（提供界面截图并加盖原厂公章） |
| c/s运维 | 支持SecureCRT、XShell、WinSCP、Mac Terminal等客户端直接连接堡垒机进行代理运维目标资产； |
| 会话分享 | ▲支持会话请求远程协助，且协同会话保持实时同步；（提供界面截图并加盖原厂公章） |
| **审计管理** | 操作审计 | 支持对用户和管理员的认证登录、操作和配置管理进行日志记录；支持改密任务的审计记录； |
| 图形协议审计 | ▲图像审计采用OCR图像识别技术，通过加载训练过的运维图片集合，可以识别图形操作中的快捷方式标题、窗口内容中的文本信息；（提供界面截图并加盖原厂公章）VNC\RDP图形协议的审计支持图像回放及指令存储两种审计形式；▲支持RDP图形操作过程中键盘输入操作记录、剪贴板和鼠标点击行为记录；（提供界面截图并加盖原厂公章） |
| 字符文件传输协议审计 | 支持字符协议SSH、TELNET和文件传输协议FTP、SFTP的协议审计，审计详细的操作指令及操作录像，同时可根据每条指令快速定位其操作录像；支持通过应用发布实现字符协议和文件传输协议的命令级审计；和图形审计的双重审计效果，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句或执行结果中关键字定位审计回放； |
| 数据库审计 | 支持通过应用发布实现数据库操作的命令级审计和图形审计的双重审计效果； |
| 全文检索 | ▲支持全文审计检索。可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯。（提供界面截图并加盖原厂公章） |
| 视频回放 | 操作过程的录像回放时，支持暂停，支持设置播放速度，支持过滤静止，方便录像的查看；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。离线回放重现维护人员对服务器的所有操作过程（回放文件下载到本地播放）； |
| 监控告警 | 支持对在线会话的实时监控和即时阻断，避免违规操作；支持对目标设备自身健康状况进行监控及告警行为； |
| 审计报表 | ▲报表针从会话、指令等多个维度进行统计；（提供界面截图并加盖原厂公章） ▲系统内置丰富报表统计模板：协议运维排名、资产运维次数top10、资产运维趋势top10、用户运维趋势top10、协议运维趋势、用户运维次数top10、指令分布top10、top10指令资产分布、指令用户分布top10、指令资产账号分布、指令排名、指令趋势、风险指令次数、风险指令top10等多种类型报表模板。（提供界面截图并加盖原厂公章）报表功能支持自定义审计查询条件，包括：时间范围、用户、资源、资源账号、IP、关键字等条件；报表导出格式支持Excel、PDF、HTML；支持邮件和FTP两种外发方式；支持报表统计历史记录； |
| **自动化任务** | 自动改密 | 自动对Windows、Linux等设备进行账号改密，可设定周期性改密； |
| 自动化运维 | ▲支持自动执行运维脚本。运维脚本分为内置和自定义两种。支持脚本类型为sh和exp两种；（提供界面截图并加盖原厂公章） |
| **部门分权** | 部门管理 | 最大支持24个层级级部门分权功能，本部门的运维管理员只能查看、管理本部门的用户和设备； |
| **系统管理** | 安全管理 | 支持HTTPS方式和Console方式进行管理； |
| ▲支持管理口与业务口分离；（提供界面截图并加盖原厂公章） |
| 虚拟化 | ▲支持对堡垒机虚拟为多台逻辑堡垒机，虚拟堡垒机之间实现独立配置、独立数据。实现IT资源的动态分配、灵活调度、跨域共享，提高IT资源利用率。（提供界面截图并加盖原厂公章） |
| 日志管理 | 支持将本机日志、告警日志通过SYSLOG、邮箱等进行外发和告警； |
| 数据维护 | 支持配置数据和审计数据的备份、自动清理，支持备份数据通过FTP方式远程备份；支持磁盘映射手动/自动清理； |
| 时间同步 | 支持配置时间同步服务器，进行时间自动校对，保障审计的有效性和准确性； |
| 网络诊断 | 支持使用ping、transroute工具对指定ip进行连接测试； |
| WEB界面 | 支持通过WEB升级系统版本、重启系统、关机； |
| **▲产品资质** | 《计算机信息系统安全专用产品销售许可证》（提供资质证明并加盖原厂公章） |
| 《信息技术产品安全测评证书》EAL3+（提供资质证明并加盖原厂公章） |
| 《IPv6 Ready Logo认证证书》（提供资质证明并加盖原厂公章） |
| **★售后服务** | 产品供应商须出具售后服务承诺书并加盖原厂公章（原件备查） |

1.3技术响应要求

1、投标方须负责完成本项目涉及的整体安装调试、服务实施等相关工作，需上门实地勘察并提供设备测试确认和理解用户原有的系统情况，否则不允许参与竞价。

2、本次项目的建设目标和服务要求，并严格根据使用单位项目进度安排完成实施工作，如有偏差由投标方负责。

3、投标商应提供投标产品对安装环境的各项要求，并且有责任检查安装现场是否符合产品安装条件。

4、供货设备的各部件、组件、配件、服务年限与服务级别必须与原厂商官网、800/400电话查询的厂商设备出厂信息一致，如未达此项要求采购方有权拒绝收货。

5、中标商在签订合同前要求必须提供证明文件，并加盖生产企业章，提供生产企业售后服务承诺函原件，证明文件和售后服务承诺函原件作为验收依据，中标后需对招标要求的技术参数逐一测试，不满足技术要求的货物将被拒收，设备出现故障后，半小时响应，1小时到达现场解决故障。

6、因部门紧急使用，如有供应商恶意参与竞价，我方有权向政采云平台投诉并取消该供应商的中标资格。

**二**.**商务要求**

1、★中标供应商须向采购单位提交终端原厂商针对本项目出具的不少于3年的免费质保与售后服务承诺函原件。提供7\*24小时问题处理, 4小时内必须排除故障。要求备件先行服务、原厂商工程师响应到场。

2、加★指标是必须满足的要求，如不满足要求，采购人有权拒绝签订合同并追究相应责任。

3、中标公司负责本项目现场安装、调试服务，需方不承担任何费用。以上设备全部提供3年质保服务。

4、所有产品要求在合同签署后15日内供货并完成安装调试，若合同签署后供应商所供货物不满足各项要求和指标，采购方有权终止合同，并且有权要求退赔。为保证售后服务的及时性，要求供货商在广东省内注册或者有服务机构。报价中包含施工，相关辅材费用等。

三.验收流程

中标供应商要针对项目验收提出与所投设备有关的完整的验收方案。

全部设备到货后，采购人对全部产品的型号、规格、配置、数量、外型、包装及资料、文件（如装箱单、保修单、随箱介质等）进行初次验收，并按照本竞价文件所列功能进行逐一验证测试。如果产品未能满足全部技术规格，采购人有权提前解除部分或全部合同并要求中标供应商赔偿相应的损失。

中标供应商应在初次验收后30天内完成所有产品的安装、配置、调试和试运行，在确保运行稳定和售后响应及时的情况下，采购人对本项目进行最终验收。

对于以上验收工作完成后产生的所有测试、验收报告必须经采购人、中标供应商共同签字盖章后方有效。

四.付款方式

本合同项下的全部货物安装调试完毕并经最终验收合格，且收到货物生产厂商针对本项目开具的《服务承诺函》后20个自然日内，甲方向乙方支付全部合同价款。

五.责任

1、若发现竞价单位存在未实质性响应文件行为，将进行废标处理，情节严重者，按照虚假竞价进行处理并记录备案。

2、若发现竞价单位存在虚假竞价行为，将在税务采购网平台列为失信供应商记录。

3、供应商参与本项目投标报价即视为响应本项目所有商务需求，否则视为无效投标。本项目面向中小企业采购,大型企业投标为无效标。