## 附件：临安国土不动产统一登记系统设备更新升级询价单

|  |  |
| --- | --- |
| **（1）内网存储** | |
| **指标项** | **产品配置要求** |
| 品牌要求 | ★非OEM品牌或联合品牌；设备制造商必须具备SNIA投票会员资格；要求签订合同前提供SNIA网站截图证明； |
| 控制器 | 配置双控制器，最大支持8控制器扩展，支持FC SAN、IP SAN和NAS组网，支持NAS功能，无需另配NAS网关，配置高速一级缓存≥64GB（缓存不包括SSD硬盘或闪存）； |
| 架构 | 全冗余架构，配置高性能冗余电源、风扇及配电模块，均可支持热插拔； |
| 接口要求 | ★配置1Gb/s iSCSI主机接口≥4个,配置10Gb/s iSCSI主机接口≥4个，配置8Gb/s FC主机接口≥8个（含光模块）；支持40Gb/s iSCSI主机接口（非InfiniBand接口）；签订合同前要求提供官网截图证明； |
| ★性能要求 | 配置高性能控制器，所投产品满足SPC-1测试IOPS≥30万，签订合同前提供SPC-1官网截图和SPC-1官网链接； |
| 硬盘要求 | 存储最大支持硬盘数（每双控）≥750；支持SSD、SAS、NL-SAS、SATA类型磁盘； |
| ★本次配置18块1.8TB 10000转企业级SAS硬盘,本次配置≧1PB存储容量授权许可； |
| 支持RAID 0、1、10、5、6等，配置硬盘容错功能，允许同一个RAID组中任意三块硬盘发生整盘物理故障；要求提供官网截图证明； |
| 快照 | 支持快照功能,单个LUN支持快照数≥2048个，有效预防各种软故障的发生；（签订合同前提供投标产品软件功能截图） |
| 数据销毁 | 支持数据一键销毁功能，可通过软件/硬件方式进行数据销毁功能； |
| 缓存 | 支持缓存加速功能许可，通过采用高性能SSD硬盘提供二级缓存功能，提高存储系统的随机访问性能，解决热点数据问题； |
| ★系统部署 | 支持基于存储底层双活功能，不需引入存储阵列之外的任何软、硬件，存储阵列自身可支持双活存储部署，将两台双控存储节点组成双活系统, 双活链路带宽最大可支持160Gb。当其中一台存储发生故障时，可自动切换到另一台存储上。切换过程自动完成，无需人工干预，业务不中断，数据零丢失。签订合同前需要提供CNAS认证机构对称双活存储系统软件测试报告扫描件或影印件； |
| 自动精简 | 支持自动精简功能，可按照实际数据存储要求，动态分配存储空间，有效保护存储空间； |
| 操作系统 | 支持Windows、Solaris、HP-UX、IBM-AIX、Linux等操作系统； |
| 管理软件 | 配置中文图形化管理平台软件，配置日志告警、指示灯告警、控制台告警、蜂鸣器告警等功能。配置高性能监控软件，要求可以实时监控CPU的利用率、磁盘繁忙程度、IOPS和吞吐量； |
| 协议授权 | 配置IPv4/IPv6协议授权，可以通过IPv4/IPv6协议进行存储访问、带外管理、远程复制等； |
| ★兼容性 | 支持国产达梦及人大金仓数据库的兼容性，签订合同前提供两家数据库厂商的对存储产品的兼容性互认证证明具备原厂双方的盖章的扫描件或影印件； |
| 为确保与VMware的兼容性，支持VMware的VAAI、VASA、SRM和VVoL四项认证；签订合同前要求提供VMware官网截图； |
| ★产品资质 | 本次招标产品通过3C认证、通过节能产品政府采购清单和环保标志产品政府采购清单，签订合同前提供3C认证、最新一期节能产品政府采购清单和环保标志产品政府采购清单复印件； |
| 售后服务 | 提供3年原厂商维保服务（包括硬件更换、软件升级等）；提供原厂商安装调试，并提供原厂商现场技术培训和现场技术指导，签订合同前提供所投标产品原厂商授权函与3年原厂质保函； |
| ★产品测试 | 此产品为数据中心业务数据运维重要产品，设备参数及性能必须满足或优于招标要求，用户方有权利要求中标方在签订合同之前对该投标产品进行测试，如虚假响应招标参数或功能要求，将拒绝签订合同、没收投标保证金并承担相应法律责任。 |
| **（2）单向光闸** | |
| **指标项** | **产品配置要求** |
| 硬件架构 | ★系统采用2+1架构，自主研发的基于安全芯片的专用隔离部件，采用单根光纤连接，保证数据单向从低安全域导入至高安全域。无操作系统，外部无法编程控制，全硬件交换, 原厂商参与《军用网络安全隔离交换产品通用要求》标准编制,要求提供相关证明 |
| 内外端机为网络协议终点，彻底阻断各种网络协议， 保证信任网络和非信任网络之间链路层的断开，彻底阻断TCP/IP协议以及其他网络协议 |
| 内外网主机系统与专用隔离部件之间采用高性PCI-E总线连接，消除性能瓶颈 |
| ★系统要求采用2U机箱设计，内外端机要求各配置不小于6个千兆电口、2个千兆SFP接口插槽，2个USB接口以及1个console管理口 |
| 内、外网分别具有独立的管理接口，而不是通过网络接口管理，也不是通过内网一个管理接口完成全部管理 |
| 内、外网分别具有独立的HA口，实现双机热备及负载均衡 |
| ★内、外网分别具有独立液晶屏，能够显示产品品牌、型号、CPU/内存占用率、网络接口状态等信息。（要求提供产品面板截图，并说明） |
| 处理性能 | 系统吞吐量≥550Mbps |
| 内部交换带宽≥5Gbps |
| 延时≤20us |
| 主模块 | ★采用基于linux内核的多核并行安全操作系统，要求提供多核并行安全操作系统证书复印件 |
| 提供基于https的图形化安全管理，支持用户名/口令、数字证书等多种认证管理方式 |
| 支持跨网段管理，实现管理终端IP地址和端口的访问控制 |
| 管理员及审计员区分并独立，支持分权管理，对管理员角色定制，可以添加多个管理员角色，并定制权限 |
| 支持管理员登录失败锁定次数、锁定时间和超时时间的设定 |
| 支持对网络接口模式进行设定（支持网闸同一侧网络接口桥模式设定或bonding设定）、MTU修改，进行灵活部署（提供证明截图） |
| 支持默认路由、静态路由及基于源地址的策略路由功能 |
| ★具有独立审计用户，支持标准Syslog日志审计方式，支持标准Syslog日志审计方式，支持高性能的syslog日志处理和存储方法的技术，并提供国家知识产权局证明文件 |
| 支持标准的SNMP协议安全管理 |
| 支持配置管理，能够对单独模块及全部模块配置进行配置导入导出 |
| 具有系统补丁管理功能 |
| 支持设备诊断信息导出（提供证明截图） |
| 支持许可证下载，方便维护管理 |
| 支持状态日志配置，通过设置硬件信息使用率进行日志记录及暂停使用 |
| 支持IP/MAC地址绑定和自动探测 |
| 通过WEB管理界面进行设备的远程关闭及重启功能 |
| 支持NTP网络时间同步； |
| 支持内外端机系统时间同步（提供证明截图） |
| ★提供调制工具，其中包括：trace、connect、tcpdump、ping、arp等（提供证明截图） |
| 支持软硬件多核技术,通过界面能够查看到多核CPU使用率（提供证明截图） |
| 提供设备运行状态检测、系统资源监控。 |
| 文件交换模块 | 支持FTP方式的文件单向导入 |
| 支持FTP文件任务和普通文件任务之间的优先级 |
| 支持FTP文件传输次数定制，保证文件单向导入的完整性 |
| 支持A网FTP用户名、密码和用户目录名的配置，保证A网不同用户传输文件的安全可靠 |
| 支持B网FTP服务状态监测，保证B网安全可靠连接到内网FTP服务器 |
| 支持专用客户端，与光闸之间通信，不需要在服务器上将文件夹共享出来，保证文件的安全性； |
| 支持客户端认证，保证文件单向导入的安全可靠； |
| 支持专用客户端，数据加密传输。 |
| 文件交换模块支持病毒检测功能，支持通过文件大小控制病毒查杀； |
| 支持多种同步模式：源端复制、源端移动、源端删除等多种模式。 |
| 支持查看任务列表，显示光闸同步文件的数量大小； |
| 支持同步任务上传，可以对比A网和B网传输文件，比较有无传输失败的文件； |
| 支持用户管理，与客户端进行认证，保证光闸文件同步任务的安全； |
| 支持任务空间限制、文件类型限制、文件数量限制。 |
| 支持优先级配置，保证重要文件任务优先传输 |
| 支持加冗传输，重要文件多次传输，最大限度的保证文件单向导入的完整性 |
| 数据库同步模块 | 支持Oracle数据库同步 |
| 不需要更改数据库结构和添加数据表，不影响数据库服务器性能 |
| ★同步由网闸主动发起并完成，不需要另外安装软件支持（要求出具原厂商证明文件及截图）。 |
| 网闸不需要开放任何服务端口，避免造成漏洞 |
| 支持一对一、一对多、多对一数据库同步 |
| 支持周期复制、实时复制、增量更新等多种同步方式。 |
| 支持设定同步时间和同步周期 |
| 支持大字段和二进制字段的数据同步 |
| 支持字段级同步 |
| 支持数据库配置任务的导入导出 |
| 支持两台单向设备实现数据库的双向同步 |
| 单向TCP | 支持单向TCP定制服务；支持源地址绑定、网络接口地址绑定功能； |
| 支持源地址、源端口、目的地址、目的端口过滤功能； |
| 支持限定一次报读数据长度限制、连续摆渡的数据报文个数限制、微妙级延时时间配置 |
| 支持任务运行标记 |
| 支持任务运行时间控制 |
| 单向UDP | 支持单向TCP定制服务；支持源地址绑定、网络接口地址绑定功能； |
| 支持源地址、源端口、目的地址、目的端口过滤功能； |
| 支持任务运行标记 |
| 支持任务运行时间控制 |
| 单向JMS | 支持JAVA平台上的信息单向通信 |
| 支持JMS监听队列配置 |
| 支持任务运行标记 |
| 高可用性支持 | 文件完整性采用“协议落地”校验机制、MD5校验、文件目录校验等多种文件完整性校验机制 |
| 防护设置 | 抗Dos攻击功能设置 |
| ICMP应答功能设置 |
| ★资质要求（提供证书复印件） | 自主创新产品证书 |
| 公安部销售许可证 （三级） |
| 3C证书 |
| 军B级军用信息安全产品认证证书 |
| ★厂家资质（提供相关复印件） | 涉及国家秘密的计算机信息系统集成资质证书（甲级） |
| 要求原厂商为应用安全联盟会员 |
| ISO1800认证证书 |
| ISO20000认证证书 |
| 国家规划布局内重点软件企业证书 |
| 厂商应为《国家电子政务外网安全接入平台技术规范》起草单位 |
| **（3）内网堡垒机** | |
| **指标项** | **产品配置要求** |
| 规格要求 | ★硬件架构——1U机架式服务器，≥6个千兆电口和1个接口扩展插槽，≥1TB存储介质 |
| ★系统安全——操作系统独立介质存储，不存于硬盘 |
| 资源授权许可 | 100个被管理IP资源授权，不限制管理员数量 |
| 性能要求 | 字符并发≥700；图形并发≥300 |
| 账号管理 | 组织架构——支持用户多级别分层管理，支持以管控方式满足大型、多级应用需求。 |
| 批量导入——支持账号的批量导入、导出和批量的修改维护操作，方便快速部署。 |
| 账号加密——投标产品能够对主、从账号的存储、传输过程进行加密； |
| 口令管理功能——系统支持被管理设备的账户口令托管，可以对被管理设备定期自动修改账户口令，并支持修改口令的密函打印,邮件发送，可以实现设备账户口令只托不管,和用户授权绑定. |
| ★自动改密——支持以计划的形式对Windows AD、linux、unix、网络设备（cisco、H3C、华为等）类资源的口令变更。（要求截图） |
| ★账号密码芯片级加密——堡垒机能够把自动更改后的密码下载到专用芯片级硬件加密设备，可通过指纹和管理权限对相应的服务器托管密码进行查看和打印等。（要求截图） |
| 认证管理 | ★认证协议——投标产品支持静态口令、动态口令、AD域、LDAP、Radius、数字证书、USBKey、MAC地址绑定等多种认证方式；（要求截图），支持静态口令、动态口令、AD域、LDAP、Radius任意两种组合的双因子认证。 |
| ★内置OTP服务器——设备自身集成一次性口令认证服务器模块，不需要再单独购买一次性口令认证服务器。（要求截图） |
| 认证加密——支持用户认证Portal页面通过SSL协议加密 |
| RDP协议NLA支持——支持windows远程桌面的网络级别身份验证。 |
| 证书管理 | 用户证书——可以从web页面下载 usb-key认证用户的个人证书 |
| ★CA证书——可以从web页面导入第三方的CA证书实现usb-key认证（要求截图） |
| ★服务器证书——可以从web页面导入替换堡垒机自身ssl服务器证书（要求截图） |
| 授权管理 | 单点登录——支持单点登录，用户通过主账号登录后，不需要再次输入身份认证信息即可直接访问其有权访问的后台资源。 |
| 系统授权功能——可细粒度授权,可根据协议实现对用户和组的交叉授权。 |
| 系统提供授权功能，并支持对系统的用户登录进行可配置的策略设置，包括限制登录IP、登录时间段等，以确保可信用户访问其拥有权限的后台资源. |
| ★分级授权——主机管理功能授权和资源访问授权。内部管理功能授权可以限制到某个树形节点的范围内； |
| 可细粒度授权,可根据协议实现对用户和组的交叉授权。（要求截图） |
| 可以基于用户、用户组、目标设备、设备组进行授权。 |
| ★身份切换代填——支持网络设备enable和unix主机su等身份切换的单点登录功能。（要求截图） |
| 系统授权功能——系统提供授权功能，并支持对系统的用户登录进行可配置的策略设置，包括限制登录IP、登录时间段（可循环，如每周五8：00-18：00时）等，以确保可信用户访问其拥有权限的后台资源. |
| 命令控制——支持命令操作的黑白名单设置，命令权限控制规则应支持正则表达式，并可以对命令的参数进行限制并记录日志 |
| ★RDP控制——对RDP的磁盘映射、剪切板（上行）、剪切板（下行）、登录console进行分别或者组合控制 |
| 双人复合操作——支持双人复合功能，运维操作时，需要通过管理员符合后方可操作。支持设备登录复合和关键命令复合。 |
| 审计管理 | 免客户端——投标产品支持统一审计功能，不需要在后台资源上安装任何审计引擎或代理程序； |
| 离线回放——可以对已经备份并在堡垒机上删除的日志进行回放审计。 |
| 审计结果展示——审计结果能够以录像重放方式展现，并支持根据时间、运维命令、进度条等方式进行定位回放；可以审计鼠标键点击操作（包括左、中、右键操作）；审计特殊按键操作（包括ctrl\alt\shift\capslock\numberlock\scrolllock） |
| 审计协议——支持Telnet、SSH、FTP、SFTP字符终端操作协议； |
| 支持RDP、VNC、Xwindow、Windows文件共享等图形终端操作协议； |
| SSH协议代理支持SecureCRT软件的Session Clone及Send To All等复杂的功能 |
| 能够审计全部操作行为，包括vi和用户shell菜单（如AIX上smit） |
| 支持AS400设备审计 |
| ★linux环境下协议代理——支持linux客户端和服务器环境下，通过堡垒机对ssh\telnet\ftp\xwin协议的运维和审计（要求截图） |
| ★扩展协议(应用发布系统)——支持自定义CS和BS类应用的自登录流程（代填密码），通过应用发布系统进行审计，例如PcAnywhere、Xmanager、数据库管理客户端、各种BS应用系统及中间件等,并且能够对使用的工具访问进行管理与控制，需详细描述管理与控制力度。 |
| ★Remote app无缝发布（应用发布系统）——全面支持微软Windows2008/2012的RemoteAPP功能，实现无缝应用发布的用户体验，所有应用发布均可本地化展示。 |
| ★数据库协议内容审计——通过应用发布服务器审计数据库时，不仅进行屏幕录像， 还可以审计数据库语句及返回值，形成文本型日志。（要求截图） |
| Imperva 产品联动——与Imperva数据库审计产品整合后，该 产品记录下的数据库输入命令都会被堡垒机所接收，并能够与堡垒机记录下的视频文件相关联，实现视频会话与命令行操作的会话关联。 |
| ★RDP图形文字识别——RDP图形文字识别并查看、检索、定位回放，独创关键技术。通过对RDP帧进行光学字符识别，进行运维内容审计。（要求截图） |
| KVM运维审计——支持KVM等带外产品的运维审计。 |
| ★密码免审计——在对从账号进行输入时，自动模糊化处理密码信息。（要求截图） |
| 内部审计——对自身全部操作进行详细的审计，并可按关键字查询和生成报表。审计结果具备较强的可读性。 |
| 日志备份——会话日志手工和定期备份、删除离线日志可审计 |
| ★日志安全——为保证日志存储的安全性，会话日志必须先备份才可以删除，不可以覆盖 |
| 外接存储——支持无内置硬盘的ISCSI外接存储。 |
| 管理员角色划分——对自身管理有角色划分，至少有系统管理员、配置管理员、审计管理员、普通用户等多种角色。各角色功能定位明晰，不可越权，支持按模块进行权限配置 |
| 实时监控阻断——系统支持事中告警功能。通过配置设置敏感操作策略，当运维用户操作这类命令，系统提供告警或者阻断，以便审计员能重点关注,告警规则支持多条命令,告警规则正则表达式 |
| 审计结果查询——提供查询界面，供用户查询某一命令或某命令的输出。可组合时间、IP、用户名、受管设备、运维协议等条件进行查询 |
| 关键字检索——对图形会话操作中的键盘输入或界面文字进行基于关键字的查询检索 |
| 报表功能——提供多角度、可定制的报表机制，可按时间、用户名、受管设备等条件组合生成报表，报表可包含运维次数、时间、大小等 |
| 报表格式——报表可导出为PDF、EXCEL、Word |
| 部署模式 | ★工作模式：物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构，不改变运维人员的运维习惯；同时支持串联接入，防止绕行。（要求截图） |
| ★HA：支持以Active-Standby方式部署（要求截图） |
| ★总控平台：总控系统可对所有的堡垒机设备进行集中管理，总控系统可以实时监控各堡垒机设备的运行状态，总控系统可对堡垒机上发生的管理事件、会话事件、告警事件进行实时或事后审计。（要求截图） |
| ★配置同步：使用一台堡垒机集中管理配置，该配置自动同步到其他堡垒机，便于大规模快速部署。（要求截图） |
| 集群模式：支持集群（多A）部署，具有很强的可扩展性，方便后期扩容。 |
| ★产品资质 | 计算机信息系统安全专用产品销售许可证（身份鉴别） |
| 涉密信息系统产品检测证书（证书内容需体现“运维”字样） |
| IT产品信息安全认证证书（证书内容需体现“运维审计”字样） |
| ★服务要求 | 产品厂家应为CNCERT网络安全应急服务支撑单位证书（国家级） |
| 计算机信息系统集成企业一级资质证书 |
| 国家信息安全服务资质认证证书\_信息安全风险评估服务一级资质 |
| 国家信息安全服务资质认证证书\_应急处理一级资质 |
| 产品成熟度达到CMMI5认证 |
| ★保修服务及授权 | 100个被管理IP资源授权及3年原厂商保修服务，出具原厂商3年售后服务承诺函及原厂商针对此项目的授权书； |
| **（4）虚拟化杀毒软件** | |
| **指标项** | **产品配置要求** |
| **架构支持** | |
| 多虚拟化平台支持 | ★虚拟化防护软件至少支持Ctrix XEN、VMWare、Hyper-V、H3C、华为、青云、EasyStack、云宏、品高等多种虚拟化平台并可在同一管理平台进行统一管理,并且具有兼容性证明或虚拟化平台厂商官方网站截图证明，并必须保证证明材料的产品名称以及公司名称与投标所使用的产品相同 |
| 多虚拟化平台导入支持 | ★虚拟化防护软件至少支持Citrix XEN、VMWare、Hyper-V、H3C、华为、等多种虚拟化平台导入，并可在同一管理平台进行统一管理提供功能截图证明 |
| Windows操作系统支持 | 虚拟化防护软件至少支持Windows Server 2003、Windows Server 2008、Windows Server 2012 Windows Server 2016版本操作系统平台的虚拟化环境。 |
| Linux操作系统支持 | 虚拟化防护软件至少支持SuSE Linux Enterprise server、Red Hat Enterprise Linux server、Oracle Linux、Ubuntu、Debian 等5个Linux服务器版本并且可以和Windows统一管理。 |
| 跨操作系统部署支持 | 对windows和linux具备相同的代理部署形式，并且具备统一管理的功能。 |
| 支持虚拟机安全策略无缝漂移 | 支持虚拟机根据实际部署需要从一台宿主机飘移到另外一台宿主机后虚拟机的安全策略不发生变化。提供功能截图证明 |
| **病毒查杀功能** | |
| 客户端病毒防护代理 | ★客户端防护代理小于100MB，有效提升虚拟化计算资源使用率。 |
| 支持错峰扫描 | 支持通过管控中心设置同时扫描最大虚拟机数量，错峰扫描，降低扫描资源占用率。并可以设置同一物理机上最大运行的查杀任务数量 |
| 支持资源占用调整 | 可配置病毒扫描时，扫描行为的资源占用率 |
| 本地缓存支持 | 支持本地杀查缓存，优化本地虚拟化环境支持。 |
| 支持通讯加密 | 支持本地代理与服务器端的通讯协议加密 |
| 支持虚拟机病毒全盘扫描 | 能够对虚拟机内部全部文件进行病毒的扫描 |
| 支持虚拟机病毒快速扫描 | 能够对虚拟机内部系统目录进行病毒的快速扫描 |
| 支持虚拟机病毒监控 | 能够对虚拟机内的文件进行进行监控，防止病毒运行 |
| 病毒扫描路径 | 支持对共享路径、U盘、光盘进行扫描 |
| 支持多种病毒查杀 | 除文件类病毒外还需支持对宏病毒、注册表病毒、内存或服务类病毒的查杀，提高虚拟化安全防护等级，对已经运行的病毒进程可以执行关闭。 |
| 支持压缩文件病毒查杀 | 支持Arj、bzip2、Cpio、CramFS、Deb、Dmg、gzip、Lzh、lzma 、lzma86、MsLZ等压缩文件格式的病毒查杀，并可以自定义添加压缩文件格式与类型 |
| 支持对未知病毒的处理策略进行配置 | 支持对未知文件进行单独处理配置忽略策略 |
| 支持对敲诈者病毒的单独策略配置 | ★可以单独配置敲诈者病毒防护功能，防止文件被加密无法打开 |
| 压缩文件查杀策略配置 | 支持对压缩文件查杀层级进行策略配置，最大可配置检查10级压缩文件，并可配置跳过一定大小的压缩文件 |
| 支持多引擎扫描 | 支持不少于3种病毒引擎扫描，并可以灵活开启关闭 |
| 支持内网云查杀 | 支持隔离网环境的私有云查杀功能以保证内网环境下的病毒查杀率 |
| 云查杀回连服务器要求 | 公有云查杀回连服务器必须为境内服务器，敏感数据不出镜 |
| 支持分组进行防火墙策略配置 | ★支持虚拟机分组防火墙策略配置，可以通过源目的IP、端口、协议进行配置优先级、阻断或允许 |
| 支持分组入侵防御策略配置 | 支持虚拟机分组入侵防御策略配置，可单独真对某组虚拟机的某类攻击规则进行开启关闭 |
| 入侵防御规则操作系统类型支持 | 入侵防御规则支持windows和linux系统的攻击特征库 |
| 入侵防御攻击规则库类型支持（windows） | windows系统攻击规则库支持拒绝服务、缓冲区溢出、木马后门、web攻击等攻击类型 |
| 入侵防御攻击规则库类型支持（linux） | linux系统攻击规则库支持提权、扫描、拒绝服务、缓冲区溢出、木马后门、web攻击等类型 |
| 入侵防御攻击规则库数量 | 入侵防御攻击规则库数量不少于2500条 |
| 支持webshell扫描功能 | ★支持对全网虚拟机进行webshell后门进行扫描，并统一展现扫描结果。提供功能截图证明 |
| webshell白名单 | 支持对webshell的文件添加白名单功能 |
| webshell扫描环境 | ★支持对windows server和linux进行webshell后门扫描。提供功能截图证明 |
| webshell后门库数量 | webshell后门库数量大于40000 |
| 支持全网虚拟机安全基线配置与检查 | ★支持对全网虚拟机安全基线进行扫描，并输出扫描结果，以打分形式呈现。提供功能截图证明 |
| windows server虚拟机安全基线扫描项 | windows server安全基线扫描项包括身份鉴别策略组、访问控制策略组、安全审计策略组、本地服务、域控、IIS、SQL、IE、Office组件 |
| linux server虚拟机安全基线扫描项 | linux 安全基线扫描项包括账号密码、SSH服务、Xinetd、kernel安全参数、core dump设置、CRON配置、ATD调度服务配置、无用文件、未授权文件的可写权限、系统守护进程的文件创建权限设置 |
| 支持安全基线一键修复 | 支持对安全基线扫描结果分组的一键修复功能，可在控制中心一键下发 |
| 安全基线定时任务 | 支持安全基线扫描的定时任务功能，可以按月、周、日、时、分，以及分组的不同维度进行计划任务扫描 |
| 支持虚拟机账号防暴力破解 | 支持分组配置虚拟机账号防暴力破解策略可以配置时间、尝试破解次数以及阻断及告警策略 |
| 支持虚拟机账号防暴力破解白名单 | 支持对防暴力破解配置白名单策略，白名单可以配置IP或IP段 |
| 支持全网虚拟机的虚拟化加固功能 | ★支持对全网虚拟机的开启虚拟化加固功能 |
| 支持虚拟化加固黑白名单 | 支持文件的黑名单、白名单 |
| 支持虚拟化加固日志统一展示 | 支持对虚拟化加固日志的详细日志展示、报表导出 |
| **管理功能** | |
| 支持虚拟化环境感知 | 支持和虚拟化平台管理中心定期感知同步，能够自动感知和保护虚拟环境的变更和迁移维护安全统一性。 |
| 支持网卡流量统计 | 支持对每一个虚拟机的网卡流量进行流量统计 |
| 支持混合式集中管控 | 支持对虚拟机和物理服务器进行统一管理，具有集中控管的功能，能够统一的管理和配置，并且相关日志能够统一的在控管平台上展现 |
| 支持分组管理 | 能够对虚拟机客户端进行分组管理 |
| 支持通讯时间间隔设置 | 能够支持设置安全终端与控制中心的通讯时间间隔 |
| 支持报表统计 | 能够对虚拟机环境的客户端安全情况进行报表统计 |
| 支持全网统一升级 | 可以通过控制中心统一下发客户端升级包到终端，并自动升级 |
| 特征库升级方式 | 特征库升级包含自动升级、手动导入的方式 |
| 支持多种升级方式 | 可以根据不同网络环境提供在线升级和隔离网升级，并提供相应工具 |
| 策略锁定 | 控制中心可锁定被防护服务器的防病毒策略，保持不被修改 |
| 开放API | 可提供开放的管理API供其他系统集成 |
| **日志报表** | |
| 日志完整性 | 记录扫描日志并包括以下字段: |
| 计算机名，上报时间，IP地址，文件名，威胁名称，扫描方式，处理结果 |
| 日志查询方式 | 提供多种日志的查看方式，包括报表；实时告警板；日志查询 |
| 报表导出功能 | 任意报表支持导出，导出格式不少于2种 |
| 虚拟化授权 | 此次要求配置8颗CPU一套 |
| **厂商资质** | |
| 销售许可证 | 具备公安部销售许可证“虚拟化杀毒”品类，并取得增强型检验结果报告 |
| ISO9001:2008质量管理体系 | 具有ISO900:2008质量管理体系认证 |
| ISCCC信息安全服务资质-应急处理服务 | 厂商具有ISCCC信息安全服务资质-应急处理服务，以保证有足够能力应对现网突发安全事件的能力 |
| CNCERT/CC网络安全应急服务支撑单位 | 厂商为CNCERT/CC网络安全应急服务支撑单位，省级或国家级 |