## 第六章　项目采购需求

## 一、货物名称及数量

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **单位** | **备注** |
| 1 | 网络准入控制 | 1 | 台 | 不接受进口 |
| 2 | 终端防病毒软件 | 1 | 套 | 不接受进口 |
| 3 | 上网行为管理 | 1 | 台 | 不接受进口 |
| 4 | 运维审计系统 | 1 | 台 | 不接受进口 |
| 5 | 虚拟专用VPN | 2 | 台 | 不接受进口 |
| 6 | Web应用防火墙 | 1 | 台 | 不接受进口 |
| 7 | 统一身份认证系统 | 1 | 套 | 不接受进口 |

## 二、技术部分

**（带\*号为必须满足的技术指标项，不满足则废标，带▲号为重要技术指标项，不满足重点扣分）**

### 1.项目背景

鹏城实验室（深圳网络空间科学与技术省实验室）建设是广东省委、省政府为深入贯彻落实党的十九大精神和习近平总书记对广东工作的重要指示，瞄准新一轮创新驱动发展需要，打造国家实验室“预备队”，建成具有全国影响力的科研机构，紧密配合国家新一代人工智能的重大规划，建设创新型广东，推进深圳率先建设社会主义现代化先行区的重大部署。

实验室以服务于国家和区域发展战略为己任，聚合国内优质创新资源，建设相关重大科学基础设施，开展跨学科、大协同的创新攻关，突破网络信息领域重大核心基础理论问题，保障国家网络空间安全，推动网络信息产业发展，引领未来学术发展方向。实验室将探索建立符合大科学时代科研规律的科学研究组织形式，积极推动粤港澳大湾区打造国际科技创新中心。

目前鹏城实验室网络安全建设设备采购设备采购处于起步阶段，在网络出口部署了抗DDOS攻击系统、防火墙、入侵防御系统等用于日常办公网络互联网访问的安全防护。

内部应用系统不断增加：OA办公系统、邮箱等应用，从阿里云落地迁移到鹏城实验室内部网络；为满足业务发展需求，已规划各类业务系统部署于内网；

安全管理越来越复杂：共建合作单位人员进驻越来越多。因此，针对物理、网络、主机、应用和数据五大部分进行安全防护建设，确保符合等保三级的规范和要求，保障系统安全、可靠、高效的运行，确保信息的机密性、完整性、不可否认性和可用性，有效避免各种潜在的威胁。

### 2、技术性能指标

#### 网络准入控制

|  |  |  |
| --- | --- | --- |
| 编号 | 招标技术指标名称 | 招标技术指标值 |
| 1 | 系统要求 | 具有独立自主知识产权，须为标准机架式硬件产品，除自身硬件设备外，产品功能的实现无需额外增加服务器等设备。 |
| 2 | 性能要求 | 2U机架结构；标准配置单电源；标准配置6个1000MBASE-T接口，可支持扩展4个1000M光口；每秒事务数（TPS)：≥9000（次/秒），最大吞吐量：≥3.3Gbps，最大并发连接数：10000（条），设备可以支持5000用户授权，本次配置2000用户授权，配置软硬件资产管理模块。 |
| 3 | 高可用性 | 准入设备必须具备HA模式，HA须支持主备机心跳IP检测及虚地址管理模式。 |
| 4 | 支持第三方监控平台，在出现重大异常情况时能及时通知网络设备放开网络。 |
| 5 | 终端部署 | **▲**准入设备应至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义部署、管理模式。（提供功能截图并加盖原厂公章） |
| 6 | 安全客户端模式部署时，客户端程序应支持功能定制，以降低系统资源耗用，提升客户端兼容性。 |
| 7 | 终端发现 | 能够实时监测并发现接入内网的PC、平板电脑、智能手机、IP设备等终端，能够在第一时间隔离阻断并通知管理员。（提供功能截图并加盖原厂公章） |
| 8 | 对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理。（提供功能截图并加盖原厂公章） |
| 9 | 准入技术 | 准入设备本身支持802.1x标准协议，无需第三方RADIUS服务器支持。 |
| 10 | 准入设备支持基于多厂商Virtual Gateway的VLAN隔离技术，实现无客户端环境下端口级准入控制，同时提供WEB重定像终端入网引导流程。（提供功能截图并加盖原厂公章） |
| 11 | 准入设备支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面，同时支持交换机接口动态VLAN下发、端口隔离模式的网络边界管理。 |
| 12 | 单台准入设备可支持至少2个核心交换机进行策略路由准入控制。 |
| 13 | 支持在IPv4和IPv6双栈环境下的终端准入控制、重定向、认证、安检、修复等。（提供功能截图并加盖原厂公章） |
| 14 | 准入设备可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。 |
| 15 | 定向引导 | 支持终端入网IE重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持http代理及多重重定向引导。 |
| 16 | 可根据用户的实际环境自定义非80端口的Web服务端口号及用户重定向引导。（提供功能截图并加盖原厂公章） |
| 17 | 能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。（提供功能截图并加盖原厂公章） |
| 18 | 具有Mac OS、Linux、iOS、Android等系统专属客户端，支持认证引导和准入管理。（提供功能截图并加盖原厂公章） |
| 19 | IP/MAC绑定 | 具有入网设备自动学习功能，支持IP/MAC/端口三者强制绑定，以及违规终端VLAN隔离机制，防止终端仿冒IP接入网络或移动设备位置。 |
| 20 | 主机防火墙 | 终端在准入通过后访问域严格受管理员策略控制。 |
| 21 | 同网段终端无法互相访问，做到精确到端口的高安全性控制。 |
| 22 | NAT设备 | 提供单独的NAT管理模块，具有NAT识别和检测机制能够及时发现网内私接的小路由器、无线AP、随身WIFI等NAT设备，通过单独的统计页面展示出其NAT设备的IP、MAC、厂商型号、接入交换机IP及端口等信息，同时能通过图形拓扑展示出NAT下连终端的类型，帮助清查通过网中网隐藏的真实网络终端。（提供功能截图并加盖原厂公章） |
| 23 | 对通过NAT入网的计算机可以实现准入控制、安全评估和修复等流程化管理 |
| 24 | Hub管理 | 能够发现内网私接的Hub、傻瓜交换机等非网管设备，当多台计算机通过Hub接入网络时，能够及时产生告警通知管理员。 |
| 25 | 准入设备能够采用VLAN隔离、逻辑关闭端口等方式禁止Hub下联计算机接入网络。（提供功能截图并加盖原厂公章） |
| 26 | 支持Hub下多个终端需分别认证才能入网和只需一台认证即可全部入网两种认证机制。 |
| 27 | 设备识别 | 支持自动识别网络设备类型，包括：交换机、防火墙等。 |
| 28 | 支持设备管理模板的定义功能，能够通过SNMP、SSH、TELNET等方式自动、批量添加网络设备。 |
| 29 | 终端网络拓扑 | 准入设备支持交换机到终端计算机的网络拓扑管理功能，能够自动绘制出网络拓扑图。（提供功能截图并加盖原厂公章） |
| 30 | 能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP表等信息。（提供功能截图并加盖原厂公章） |
| 31 | 支持在界面上提供对该网络设备进行TELNET、SSH等管理。（提供功能截图并加盖原厂公章） |
| 32 | 交换机状态展现 | 支持可网管型交换机面板图形化展现各接口状态（up、down、trunk等），以及各接口下联的终端详细信息（IP、地址、MAC地址等）。 |
| 33 | 能够支持自上而下逐级查找终端的具体位置、安全状态、认证用户、上下线时间等信息。 |
| 34 | AP联动管理 | 能够与主流的AP设备深度联动，支持AP控制器面板的图形展现，包括AP连接状态、下联终端信息（IP地址、MAC地址等）等。 |
| 35 | DHCP中继 | 能提供稳定的DHCP服务，并可以通过DHCP二次地址分配机制实现安全准入管理，支持交换机中继认证方式。支持DHCP服务器筛选，防止非法DHCP服务器分发错误地址。 |
| 36 | 能够根据用户、IP/MAC绑定信息等条件，为指定终端设备分配特定的IP地址。 |
| 37 | 支持DHCP服务器筛选，防止非法DHCP服务器分发错误地址 |
| 38 | 终端识别 | 支持当前主流智能终端设备的安全准入控制，能够自动识别主流手机、智能终端等设备。 |
| 39 |
| 40 | 移动终端入网 | 提供独立的智能终端入网引导界面的自主定制功能，至少包括界面标题、界面LOGO、界面说明文字等。 |
| 41 | 能够提供移动终端入网的设备注册功能。（提供功能截图并加盖原厂公章） |
| 42 | 认证检查 | 苹果应用商店提供支持iOS的安全准入app下载安装；支持Android客户端自动生成，以及自动签名等功能。 |
| 43 | 可提供手机或智能终端强制VPN拨号认证管理。 |
| 44 | 支持基于Android系统对安全管家、金山手机卫士、NQ Mobile Security、瑞星手机安全软件等安全应用程序的状态安全检查（提供功能截图并加盖原厂公章） |
| 45 | 支持进行基于Android的安装软件、运行进程等的安全检查。（提供功能截图并加盖原厂公章） |
| 46 | 联动认证 | 能够全面结合用户已有的认证或业务系统，可以与RADIUS、LDAP、STMP/POP等采用标准协议的系统做深度联动认证。 |
| 47 | AD域单点登录 | 能够与用户现有的AD域相结合，当用户登录到AD域后，无需二次认证即可入网，避免多次认证的繁琐流程。 |
| 48 | 当用户未登录到AD域时，该终端将一直被隔离，该状态下只有通过IE页面进行认证才能够入网。 |
| 49 | 短信认证 | 支持短信认证模式，用户在登记入网手机号码后，能够在手机上接收到入网的短信验证码，并在IE页面上利用短信验证码认证入网。 |
| 50 | 来宾管理 | 能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长，提供临时入网码，支持来宾设备与受访人员进行一对一绑定功能，并可以生成对应的审计报表。 |
| 51 | 接入审核 | 能够针对不同的角色或设备类别有选择的开启入网审核功能，待审核的用户或设备必须经过管理员审批才能入网。 |
| 52 | 安全检查库 | 准入设备须提供系统安全配置、用户行为规范等类别检查项，至少提供25种以上安全检查项。 |
| 53 | 系统补丁 | 准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分类、补丁分发、补丁报表等功能。 |
| 54 | 能够在IE页面进行入网终端的补丁检查，补丁均划分为严重、重要、中等的类别，能够在IE页面显示出检查结果。 |
| 55 | 防病毒软件 | 支持基于IE页面的杀毒软件状态检查，支持杀毒软件版本、病毒库和运行情况的检查，支持20种以上主流杀毒软件检查，。 |
| 56 | 安全配置检查 | 支持windows密码策略、屏保、共享目录、弱口令、防火墙、网卡配置等项进行检查和修复。 |
| 57 | 健康性检查 | 能够对终端的磁盘使用率、垃圾文件、IE主页、网络监听端口等安全性配置进行检查和修复。 |
| 58 | 客户端检查 | 能够检查主流桌面管理系统（包括Landesk、北信源、威盾、盈高、圣博润等）客户端是否安装及正常运行，支持客户端强制安装。 |
| 59 | 自定义安全检查 | 能够对终端文件的路径、版本、大小、MD5、进程、注册表项、服务等项自定义组合检查。 |
| 60 | 能够通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表等方式进行安全修复。（提供功能截图并加盖原厂公章） |
| 61 | 终端安全加固 | 能够通过傻瓜式的漏洞修复模式为用户提供简单、形象的漏洞自我修复功能，完全不需要管理员的介入即可完成终端安全风险项修补。 |
| 62 | 软件检查 | 通过安全检查检测终端软件安装、使用状态； |
| 63 | 自动强制为终端安装软件； |
| 64 | 软件产品授权，支持进行windows、office、WPS的产品授权信息进行检查（提供功能截图并加盖原厂公章）。 |
| 65 | IP地址管理 | 提供IP地址分配表，能够通过图示直观的查看各网段中未分配、开机、关机的数量和分布情况。 |
| 66 | 能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的IP使用情况。 |
| 67 | 能耗管理 | 提供未关机终端自动统计功能，并能够按照部门、时间段等条件生成统计报表。 |
| 68 | 移动端设备管理 | 移动端管理平台可实现设备快速定位、设备审核、实时报警监控、小助手确认码生成、准入控制器管理、平台基本信息、关机与重启（提供功能截图并加盖原厂公章） |
| 69 | 管理角色控制 | 准入设备须采用系统管理员、安全管理员、审计员三权分立机制，防止单个角色管理者权限滥用。 |
| 70 | 网络诊断工具 | 支持通过Web管理界面提供ping、抓包、traceroute、nslookup等功能，并可以设置命令参数进行相关调试。 |
| 71 | 消息群发 | 能够支持在指定的一台或者多台终端计算机上产生桌面消息通知，该消息会立即弹出在用户桌面上，对用户进行提醒。 |
| 72 | 资产管理 | 能够对全网计算机上安装的软件进行统计，可以按照部门、名称提供精确查询以及软件资产报表的导出； |
| 73 | 能够对终端硬件初始记录、最新记录和变动记录形成报表，并且能够查询变动的历史； |
| 74 | 准入设备能够针对软硬件资产变动、资产异常情况提供了丰富多样的报警方式，便于管理员及时迅速了解资产信息。 |
| 75 | 软件分发 | 准入设备应具有软件分发和部署功能，管理员可以预定义软件分发的路径、运行参数、是否执行等任务策略，以提升软件部署效率。 |
| 76 | 能够自动判断并统计软件分发、部署的成功率，支持进程、注册表、安装路径等多种参数的组合判断。 |
| 77 | 安全管理报表 | 准入设备后台能够按周、月、年统计安全状况走势图； |
| 78 | 准入设备后台提供每日入网报告、每周入网报告、每月入网报告。 |
| 79 | 报警信息 | 可以提供紧急、重要、次要、提示等多个级别自定义报警模式； |
| 80 | 支持系统报警、网络报警、终端报警等类别，超过20种以上自定义报警类型； |
| 81 | 支持Syslog报警信息的定向输出。 |
| 82 | 报警提醒 | 准入设备能够以邮件、手机短信、页面消息等多种报警方式提醒管理员各种安全异常状态。 |
| 83 |
| 84 | 第三方产品联动 | 支持与主流上网行为管理系统深度联动，构建内网准入、准出的全面安全管理体系； |
| 85 | 能够与主流动态口令认证系统相结合，提供动态密码联动认证机制； |
| 86 | 支持与国内外主流U-Key联动认证。 |
| 87 | 售后服务 | 中标后提供原厂三年售后服务承诺函。 |
| 88 | 资质要求 | 具有公安部《计算机信息系统安全专用产品销售许可证》 |
| 89 | 具有国家保密局《涉密信息系统产品检测证书》 |
| 90 | 具有国家版权局《计算机软件著作权登记证书》 |
| 91 | 具有国家密码局《商用密码产品销售许可证》 |
| 92 | 具有国家知识产权局产品专利2项及以上 |

#### 终端防病毒软件

|  |  |  |
| --- | --- | --- |
| 编号 | 招标技术指标名称 | 招标技术指标值 |
| 1 | 环境要求 | 控制中心采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能 |
| 2 | 支持以下操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10等Windows客户端 、Windows Server 2008 R2/2012/2012 R2/2016等Windows服务器系统；SUSE/Red Hat/CentOS/Ubuntu等Linux系统 |
| 3 | 终端授权 | 提供2000个支持Windows XP/VISTA/WIN7/WIN8/WIN10等客户端的授权，包含防病毒功能、补丁管理功能、运维管控功能、移动存储管控功能、XP系统防护功能和终端审计功能，其中终端审计包含统计软件运行的活动状态、外设使用日志、开关机日志、系统帐号日志、文件操作日志、文件打印日志、邮件日志等功能；提供3年售后服务，软件升级 |
| 4 | 提供50个支持Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012等Windows服务器系统的防病毒功能授权；提供50个支持SUSE/Red Hat/CentOS/Ubuntu等Linux系统的防病毒功能授权；提供3年售后服务，软件升级 |
| 5 | 资产管理 | 支持发现设备的IP-MAC地址的绑定（提供产品界面截图并加盖原厂公章） |
| 6 | 支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件（提供产品界面截图并加盖原厂公章） |
| 7 | 终端策略管理 | 支持对终端桌面系统的账号密码策略（账号锁定时间、密码复杂度、密码最长使用期限、检察周期）、本地安全策略（注册表、文件共享、系统还原）、控制面板策略（用户账号、添加删除程序、网络和共享中心、管理工具）、屏幕保护（屏保开启及等待时间）、桌面壁纸（强制壁纸）、浏览器安全、杀毒软件检查 |
| 8 | 病毒、恶意代码、木马防护 | 支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件； |
| 9 | 支持手工导入MD5+SHA1的黑白名单方式，支持txt批量导入方式；（提供产品界面截图并加盖原厂公章） |
| 10 | 对敲诈者病毒提供防护机制，同时可提供相关解密工具；（提供功能截图并加盖原厂公章） |
| 11 | 具备与国产操作系统（包括中标麒麟、红旗、普华、龙芯）的兼容性证明文件（提供厂商认证证书复印件） |
| 12 | 补丁分发与漏洞修复 | 产品支持检测过期补丁，智能屏蔽不支持操作系统的补丁；具备漏洞自动修复、定期修复、按时间段修复，并具备蓝屏修复功能;**（**提供系统截图证明并加盖原厂公章**）** |
| 13 | 产品漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端P2P补丁分发加速，有效节省外网带宽资源。 |
| 14 | 功能扩展 | 可支持功能扩展，如运维管控、移动存储介质管理、软件管控、软件管理、数据防泄漏、网络准入等。 |
| 15 | 违规外联与接口控制 | 违规外联发生时可针对内外网连接状态分别设置违规处理措施 |
| 16 | 支持接口控制：USB接口、串口、并口、1394等，光盘控制：读取权限、刻录权限，设备控制：USB移动存储类、USB非移动存储、蓝牙、打印机、冗余硬盘、键盘、摄像头、扫描仪、手机平板等 |
| 17 | 设备联动 | ▲配置与下一代防火墙设备联动，达到网关边界联动防御效果（提供产品界面截图并加盖原厂公章） |
| 18 | 资质要求 | 提供公安部颁发的《计算机信息系统安全专用产品销售许可证》； |

#### 上网行为管理

|  |  |  |
| --- | --- | --- |
| 编号 | 招标技术指标名称 | 招标技术指标值 |
| 1 | 硬件规格 | 机架式独立硬件设备，系统硬件为全内置封闭式结构，稳定可靠，加电即可运行，启动过程无须人工干预。 |
| 2 | 至少支持12个千兆电口、12个千兆光口、4个万兆光口，接口无路由/交换/LAN/WAN等固化区分，均可作为二三层接口使用，支持多桥组部署 |
| 3 | 性能 | 最大网络吞吐≥30Gbps，并发连接数≥600万，每秒新建连接数≥100万，支持用户数≥1.6万人 |
| 4 | 部署适应性 | 支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备 |
| 5 | 支持源地址转换、目的地址转换、双向地址转换、NAT44，支持DDNS功能， |
| 6 | 支持静态路由、策略路由、RIP、OSPF、ISP路由，其中ISP路由支持自定义，并可提供基于应用的策略路由 |
| 7 | 接口默认属于root，创建VRF后可把接口添加到VRF内，一个接口只能属于一个VRF； |
| 8 | 支持4G扩展网卡。支持在4G接口上运行IPSec VPN。 |
| 9 | 功能要求 | 实际配置支持一对一、多对一、多对多等多种形式的NAT，支持H.323等应用协议ALG |
| 10 | 实际配置支持基于用户、应用、时间对象的流量管控和策略设置接口，实际配置支持second IP地址 |
| 11 | 支持基于源、目的、规则集的入侵检测，支持5种自定义动作 |
| 12 | 支持针对Web服务器防护，包括网页防爬虫、网页防篡改、HTTPS防护、DDoS攻击防护、Web攻击过滤、漏洞防护自学习等 |
| 13 | 系统定义超过3000条规则，包含Backdoor、bufferoverflow、dosddos、im、p2p、vulnerability、scan、webcgi、worm、game。 |
| 14 | 配置IPSec隧道授权≥512个 |
| 15 | IPsec VPN支持第三方对接和快速配置，自有设备对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址，支持配置国密 |
| 16 | 支持配置IPsec VPN隧道内网段映射，解决VPN地址网段重叠问题 |
| 17 | 支持自定义关键字对象，在应用控制的时候可选择“包含”、“等于”、“不等于”、“大于”、“小于”五种匹配模式，匹配类型包含关键字和数字， |
| 18 | 支持HTTPS解密功能，支持页面及命令行配置解密策略，包括入接口、源地址对象、目的地址对象、https对象、域名排除等。支持针对HTTPS网站、HTTPS搜索记录、HTTPS邮箱等内容进行审计；HTTPS邮箱支持审计主题、内容、附件等；支持HTTPS域名库，预定义域名以及自定义域名 |
| 19 | 支持即时通讯应用管控的精细化管理，可管控微信的“位置分享”、“朋友圈”、“附近的人”、“朋友圈”、“摇一摇”、“漂流瓶”、“发文件”、“发消息”、“视频语音”、“登陆注销”等行为 |
| 20 | 支持WEB Portal认证功能，支持本地认证、Radius认证、LDAP认证 和LDAP用户同步，支持对接IMC、AAS、SAM等常见AAA服务器，支持配置强制重新认证间隔，支持配置认证通过后重定向URL，要求本机自身支持短信认证功能 |
| 21 | 支持单用户全天行为分析报表，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息 |
| 22 | 支持认证页面自定义 |
| 23 | 支持微信认证功能，使用微信连WiFi2.0接口，限制微信流量放通（pc和移动端，认证通过放通），支持基于http获取access\_token，支持微信内部浏览器http弹portal, 强制关注功能（定时检查用户是否关注公众号） |
| 24 | 支持自新建、移动、删除和搜索用户、用户组，支持模糊搜索用户名、用户组名 |
| 25 | web管理界面支持Ping、Traceroute、TCP Syn诊断工具，可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析 |
| 26 | 支持命令行、界面管理端口的漂移 |
| 27 | 支持本地日志记录和远程日志输出； |
| 28 | 支持专用的日志审计管理软件 |
| 29 | 其他 | 支持本地生成用户终端上下线、上网日志、普通内容、AP资料、场所资料、虚拟身份、搜索关键字信息、BBS信息、Email信息等数据库表； |
| 30 | 至少支持任子行、派博、爱思、虹旭、锐安、网博、中新、恒邦、兆物、云辰、宽广智通、携网等主流后端公安平台的直接对接，并提供应用与平台代码关系对照 |
| 31 | 支持烽火、普天、长虹、海信等胖AP的用户溯源审计； |
| 32 | 支持数据实时上报，同时可根据用户要求设置上报时间周期； |
| 33 | 支持与标准的电信CRM系统进行对接，可主动获取场所和AP等信息； |
| 34 | 支持FTP、FTPS、HTTP、UDP等方式传输 |
| 35 | 支持.ZIP、.syslog、.XML、.bcp、.ok等文件格式 |
| 36 | 支持标准的CBC模式的DES加密算法 |

#### 运维审计系统

|  |  |  |
| --- | --- | --- |
| 编号 | 招标技术指标名称 | 招标技术指标值 |
| 1 | 产品形式 | 专用安全操作系统，软件镜像形式 |
| 2 | 硬件参数 | X86架构，提供1000个设备管理授权 |
| 3 | 部署方式 | 物理旁路，逻辑串联模式，不影响正常业务流量 |
| 4 | 支持基于水平可扩展的集群化架构设计与部署，支持跨地域、跨数据中心，多层次部署 |
| 5 | 支持NAT地址映射部署，通过映射后的IP地址访问堡垒机 |
| 6 | 资源管理 | 支持SSH、RDP、VNC、Telnet、FTP、SFTP、DB2、MySQL、Oracle、SQL Server等协议 |
| 7 | 支持对主机地址进行精确搜索，支持资源自动发现，可自动发现设置的IP范围内的资产，并且可以指定端口，支持FTP协议，并可以使使用FlashFXP、FileZilla等常用的FTP工具，支持SFTP协议，并可以使用WinSCP、FlashFXP、xftp等常用工具 |
| 8 | 支持云主机资源批量添加，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure云平台的资源（提供功能截图并加盖原厂公章） |
| 9 | 可通过应用发布实现对MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client类型等应用程序/客户端的扩展支持 |
| 10 | 支持不同的资源使用相同的IP或域名 |
| 11 | 支持内置常用的系统类型，包括Linux、Windows、H3C、Huawei、Cisco |
| 12 | 支持资源按标签管理，每个用户可以给每个资源打10个标签、支持批量添加和删除标签 |
| 13 | 支持TELNET、SSH协议资源使用普通账户自动切换到root（或enable）账户 |
| 14 | 堡垒机系统版本支持PC版本与手机APP版本（提供功能截图并加盖原厂公章） |
| 15 | 支持无需安装任何客户端使用MAC OS系统Safari浏览器登陆堡垒机系统进行运维管理（提供功能截图并加盖原厂公章） |
| 16 | 资源运维 | 支持SSH、RDP、TELNET、VNC协议资源的批量登录功能，支持SSH客户端、FTP客户端、SFTP客户端访问目标资源 |
| 17 | 提供类似云盘形式的文件存储，支持RDP、SSH、VNC协议类型主机的文件上传和下载，并进行审计 |
| 18 | 支持通过Web页面访问目标支持包括SSH、RDP、TELNET、VNC和应用发布资源，支持SSH key方式登录SSH资源，支持多台SSH、TELNET协议资源批量执行操作指令，支持将运维资源列表导出成xshell和SecureCRT格式的配置 |
| 19 | 支持Xshell、putty、MAC terminal等客户端和Remote Broswer（HTML5）访问目标资源，支持双人授权和多因子认证，运维资源可分页显示，并且可以根据名称、IP、标签等多种条件进行查找 |
| 20 | 用户管理 | 支持本地、RADIUS和AD域等认证类型，支持通过设置来源IP控制和访问时段控制，限制用户访问堡垒机 |
| 21 | 支持用户的IP地址（黑名单或白名单）和MAC地址限制（黑名单或白名单）限制，非法地址无法登陆 |
| 22 | 支持访问控制策略按部门分权，不同部门的配置管理员只能针对自己部门及自己直属子部门设备进行访问权限设置；支持密码修改计划部门分权，使得不同部门的密码保管员只能修改/保管自己部门的设备上的帐号密码；支持审计功能按部门分权，使得不同部门的审计管理员只能审计自己部门、自己直属子部门设备上的操作日志 |
| 23 | 访问策略与动态授权 | 无需安装任何客户端，便可单点登录RDP、VNC、Telnet、SSH等协议和应用发布的远程资源 |
| 24 | 命令权限控制动作包含拒绝执行、允许执行、告警、动态授权和断开 |
| 25 | 堡垒机本身预制主机和网络设备的基本命令，用户可根据特定场景需要进行自定义命令 |
| 26 | 访问控制策略基于用户、用户组、资源账户、账户组、有效期、文件管理控制、文件传输控制（上传、下载）、RDP剪切板控制、时间限制、IP限制进行设置 |
| 27 | 访问控制策略支持配置双人授权候选人，针对核心设备，需要管理员现场审批才能操作 |
| 28 | 支持命令控制策略中对操作命令支持正则表达式和通配符方式设置匹配规则 |
| 29 | 自动运维 | 支持对SSH协议资源进行账户同步，包括推送账户（将堡垒机账户同步到对应资源）、拉取账户（将对应资源的账户与堡垒机本身做对比） |
| 30 | 支持运维任务，通过编排步骤的方式，自由组合命令、脚本和文件传输步骤，实现灵活的自动化运维任务 |
| 31 | 工单管理 | 工单支持多人多级审批，最大支持5级审批 |
| 32 | 工单审批时，可以设置多人审批模式或会签审批模式 |
| 33 | 支持文件管理权限、RDP剪切板权限、上传、下载权限的申请 |
| 34 | 操作记录 | 支持H5页面展示当前操作用户的登录名水印 |
| 35 | 支持字符协议SSH、TELNET和文件传输协议FTP、SFTP的审计，详细记录操指令和操作指令的执行结果 |
| 36 | 对录屏日志，可根据文本审计的内容为关键字进行图形搜索，搜索出来的结果可以直接定位到相关图形画面进行回放（提供功能截图并加盖原厂公章） |
| 37 | 支持双人授权审计和协同用户审计，支持系统内置多种系统报表和运维报表模板，支持按日、周、月为周期，自动生成报表 |
| 38 | 即可对FTP协议进行审计，还可以对堡垒机自身的文件上传和下载的功能的执行可以被审计 |
| 39 | 会话回放 | 支持在线回放过程支持播放速度调整、拖动、暂停、停止、重新播放等播放控制操作 |
| 40 | 支持离线回放重现运维人员对资源的所有操作过程，并支持回放文件下载到本地播放 |
| 41 | 可根据文本审计的内容为关键字进行图形搜索，搜索出来的结果可以直接定位到相关图形画面进行回放 |
| 42 | 改密计划 | 可以根据从账户、时间、改密周期、改密方式生成详细的改密计划，到期自动执行 |
| 43 | 支持修改数据库账户的密码，包括DB2、MySQL、Oracle、SQL Server |
| 44 | 改密方式可以支持随机生成不同密码、随机生成相同密码、手动指定相同密码并支持自动改密结果发送到指定改密计划的管理员邮箱 |
| 45 | 改密策略支持基于资源账户、账户组、改密方式、执行方式进行设置 |
| 46 | 支持查看改密日志，了解改密账户总数、改密成功数量、改密失败数量和未修改数量 |
| 47 | 系统维护 | 支持全量或者增量方式进行系统备份，支持通过导入升级包的方式一键升级 |
| 48 | 支持系统登录次数和资源运维次数的按周和按月展示趋势图，支持系统状态和系统信息展示 |
| 49 | 支持用户多次登录失败将自动锁定账户或IP，可配置解锁时长、到期自动解锁，也可以手动解锁 |
| 50 | 支持微信小程序手机令牌（提供功能截图并加盖原厂公章） |
| 51 | 支持绑定SSH公钥，实现免密码登录 |
| 52 | 支持修改系统自身对外提供服务的默认端口 |
| 53 | 支持配置和数据自动备份到远程FTP、SFTP服务器存储 |
| 54 | 支持系统负载、内核信息、内存信息、网卡信息、磁盘使用信息、路由表信息、ARP表信息等运行状态信息的采集 |
| 55 | 产品资质 | 产品具备《计算机信息系统安全专用产品销售许可证》 |

#### 虚拟专用VPN

|  |  |  |
| --- | --- | --- |
| 编号 | 招标技术指标名称 | 招标技术指标值 |
| 1 | 设备性能 | 移动安全接入性能≥300Mbps，移动终端安全支持接入数≥1600个，移动终端接入速率≥180个/秒；千兆电口≥6个，单电源，标准1U架构，配置1000个企业移动管理接入授权，500个SSL VPN接入授权 |
| 2 | 部署方式 | 支持网关模式、单臂模式、双机模式、集群模式的部署 |
| 3 | 基本特性 | 专业VPN设备，采用标准SSL、TLS 协议，同时支持IPSec VPN、SSLVPN两种VPN，非插卡或防火墙带VPN模块设备。 |
| 4 | 支持Windows、IOS、Android、塞班、黑莓等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入，或通过PPTP、L2TP VPN方式接入； |
| 5 | 支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows EDGE，Google Chrome，Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用。（提供截图证明并加盖原厂公章，或现场演示） |
| 6 | 易用性 | 可支持虚拟门户功能，在一台设备上配置不同的访问域名、IP地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果； |
| 7 | 支持智能递推技术，针对多外链的门户网站进行动态嗅探页面内的链接并完成资源自动授权，防止资源漏访；支持Web参数修正，可针对Flash、Java、Applet、或视频播放器对象所引用资源路径进行修正，避免无法播放的问题。 |
| 8 | 权限控制 | 支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定 |
| 9 | 身份认证 | 产品必须支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证 |
| 10 | 高速性 | 支持至少4条以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠SSLVPN设备同样可实现SSLVPN接入用户的多线路自动优选功能 |
| 11 | 支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。（提供界面配置截图或提供自主知识产权证明） |
| 12 | 移动APP集成 | 支持自助式App Warpping封装，不需要移动安全厂商协助，移动办公App快速上线(提供截图证明并加盖原厂公章) |
| 13 | VPN SDK 支持Ticket认证API接口实现VPN免密单点登录，并提供API接口，支持工作App自助修改密码 |
| 14 | 高管理要求 | 支持15级以上用户组树形结构分级管理，下级组可继承上级组的角色，资源及认证方式等属性 |
| 15 | 支持15级以上的管理员分级分权限管理，从Admin派生树形结构下级管理员；上级管理员可分配下级管理员享有设备配置模块权限，可管理的用户、资源、角色权限，并可限制下级管理员是否允许创建下级管理员、创建资源、创建角色；上级管理员可限制下级管理员对权限内配置享有查看或配置权限 |
| 16 | 支持针对移动APP的VPN安全代码的自动封装，实现App应用的安全加固（提供界面截图证明） |
| 17 | 移动智能终端支持 | 产品支持应用虚拟化功能，可以无需二次开发，即把Windows应用发布到移动智能终端中 |
| 18 | 产品应该支持企业级“云盘”（又名“网盘”、“文件共享”）功能， |
| 19 | 支持改写WindowsRDP协议，经改写的协议必须独立于OS运行环境，避免跨平台兼容性，针对图像数据，服务端必须支持有损压缩算法； |
| 20 | 防火墙 | 产品应具备基于状态监测技术的防火墙功能，能够抵抗常见的网络攻击 |
| 21 | 产品及企业资质 | 提供原厂商售后服务体系ISO9001认证证书 |
| 22 | 提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》 |
| 23 | 提供产品IPV6 Ready认证证书，并在全球IPV6测试中心官网可查 |

#### Web应用防火墙

|  |  |  |
| --- | --- | --- |
| 编号 | 招标技术指标名称 | 招标技术指标值 |
| 1 | 配置要求 | 系统应为机架式独立硬件设备，全内置封闭式结构，具有完全自主知识产权的专用安全操作系统，稳定可靠，2U机架式设备，标配6个千兆自适应电口，2个万兆光口，硬盘不低于1TB，支持扩展槽 |
| 2 | 性能要求 | HTTP吞吐：4000M；HTTP新建(CPS)：36000/s；最大并发数：1000,000； |
| 3 | 网络部署 | 支持透明流模式、透明代理模式、反向代理模式、路由牵引模式、镜像检测模式及镜像阻断模式 |
| 4 | 应支持多服务器的负载均衡，工作在网关模式，对保护的多台负载WEB服务器，达到平均分发、按比例分发、负载分摊、响应比分摊等多种负载均衡模式。应至少支持IP哈希、URL哈希、轮循算法、权值等算法。 |
| 5 | 牵引防护 | 支持通过BGP方式对流量进行牵引，并在清洗攻击后回注，回注过程支持设置SNAT策略 |
| 6 | 网络安全 | 支持静态及动态ARP管理，支持静态路由和策略路由管理，提供DNS服务器功能，支持服务器泛域名和普通域名服务 |
| 7 | 支持静态及动态黑白名单策略，包括IP及URL黑白名单，支持基于源目的IP、端口服务和时间等元组的包过滤功能 |
| 8 | Web安全防御 | 支持HTTP协议校验，可根据实际网络状况自定义协议参数合规标准，过滤非法数据 |
| 9 | 支持HTTP访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则，过滤非法请求 |
| 10 | 支持HTTPS防护，支持上传证书及密钥 |
| 11 | 应能识别和阻断注入攻击，支持防扫描陷阱，支持爬虫防护，支持文件上传、下载过滤，支持LDAP、XPATH、struct2/xworks检测和防护 |
| 12 | 应能识别阻断跨站脚本(XSS)注入式攻击，应能识别阻断盗链攻击，应能识别阻断跨站请求伪造攻击，非法上传检测阻断，包括恶意WebShell防护，对网页请求/响应内容中的非法关键字进行检测、过滤 |
| 13 | 虚拟补丁 | 支持虚拟补丁功能，支持导入appscan等第三方扫描器的扫描结果生成WAF的规则，对此类网站漏洞直接防护 |
| 14 | 智能部署 | 支持网站自学习建模，可通过学习URL、host等信息展示网站结构树形图，并支持对URL的访问量和响应健康度进行图形化统计（提供功能截图并加盖原厂公章） |
| 15 | 支持通过自学习的URL参数的长度、类型、范围及请求方法等数据特点创建黑白名单模型，如果参数违反模型则判断为非法流量，直接执行阻断或封禁动作（要求提供功能截图并加盖原厂公章） |
| 16 | 支持自定义防护模板，提供通用、增强、专家的初始防护策略模板 |
| 17 | 一键断网 | 支持通过移动终端管理，实现网站快速应急处置； |
| 18 | 支持网站批量离线、网站批量恢复、网站一键断网、网站一键恢复操作（提供功能截图并加盖原厂公章） |
| 19 | 威胁情报支持 | 支持第三方威胁情报库更新 |
| 20 | 支持利用安全情报规则进行防护，并支持基于威胁情报的日志查询（提供功能截图并加盖原厂公章） |
| 21 | 网页防篡改 | 能进行配置自动分发功能，应采用内核级防篡改保护，能及时阻止并报告攻击事件；应支持支持超过40GB以上网页防篡改保护和恢复功能 |
| 22 | 应至少同时支持Windows、Linux、AIX三个操作系统的的网页防篡改；（提供功能截图并加盖原厂公章） |
| 23 | 应能支持对所有安装防篡改客户端的服务器进行集中管理，能监控所有服务器状态、防篡改信息 |
| 24 | DDoS防护 | 支持检测并清洗的攻击类型包括但不限于： |
| 25 | Land、Winnuke、Smurf等；TCP（SYN、SYN-ACK、ACK、RST、FIN等）；UDP（各种端口扫描、Flood等）；ICMP（不可达，Flood等)；DNS Query Flood、HTTP GET Flood、HTTP Post Flood、CC等 |
| 26 | 云防护联动 | 支持与云防护中心进行联动，并在WAF本地进行云端配置管理（提供功能截图并加盖原厂公章） |
| 27 | 支持在WAF本地查看云中心访问流量及防护攻击量统计 |
| 28 | 审计及告警 | 要求至少具备独立的审计日志、流量日志、攻击日志、网页防篡改日志、DDoS防护日志及威胁情报日志模块，且支持按不同日志分类进行syslog外发，至少支持字符串和json两种数据格式 |
| 29 | 支持日志可视化，可对访问日志、攻击日志及安全情报等日志进行二次分析，并通过饼图、曲线图及柱图等对分析结果进行图形化统计 |
| 30 | 要求至少支持日志、trap、邮件、短信等告警方式 |
| 31 | 监控及报表 | 支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标服务器、攻击类型、攻击趋势、流量趋势及实时事件的动画统计 |
| 32 | 态势监测支持对监测范围、防护区域和防护对象的自定义设置 |
| 33 | 系统须能够对遭受攻击按照攻击次数、防护的网站、遭受攻击的网页、攻击类型、攻击时间（或发现攻击的时间）等进行统计并排名 |
| 34 | 能够根据网站的访问防护的网站、被篡改内容、篡改内容的类型、试图进行的篡改、成功的篡改、发现的日期、事件发生的日期等条件进行详细信息的查询 |
| 35 | 管理界面 | 支持HTTPS、SSH、Console、WebShell多种管理方式 |
| 36 | 支持Web管理端口自定义 |
| 37 | 产品资质 | 产品具有《IT产品信息安全认证证书》，且该证书产品技术标准为《WEB应用防火墙产品安全技术要求》，提供证书复印件证明。 |

#### 统一身份认证系统

|  |  |  |
| --- | --- | --- |
| **编号** | **招标技术指标名称** | **招标技术指标值** |
|  | 组织机构管理 | 从 HR系统同步机构数据 |
|  | 管理HR和非HR机构数据 |
|  | 成建制划转操作，例如：机构转移、机构合并等（提供功能截图并加盖原厂公章） |
|  | 同时对多套组织机构数据进行管理（提供功能截图并加盖原厂公章） |
|  | 灵活扩展组织机构的属性定义，并支持定义多值属性 |
|  | 灵活配置从HR等系统回收的组织机构属性及其映射关系 |
|  | 灵活配置从HR等回收属性的静态动作或动态动作 |
|  | 允许对回收操作的过程进行定义、监控及错误后可进行重试（提供功能截图并加盖原厂公章） |
|  | 支持批量操作，并支持预导入功能 |
|  | 用户管理 | 基于组织机构的用户查询，包含树形的、扁平的； |
|  | 从HR系统同步用户数据 |
|  | 手工和批量管理非HR用户数据 |
|  | 对用户的入职、信息变更、禁用、启用、逻辑删除、离职等进行操作 |
|  | 多种用户类型的扩展，例如：HR用户、非HR用户、临时用户 |
|  | 用户类型间实现互转(HR转非HR，非HR转HR) |
|  | 统一用户名的属性在多种规则范围内可修改（提供功能截图并加盖原厂公章） |
|  | 用户组管理，以及用户组内人员的灵活管理 |
|  | 灵活扩展用户的属性定义，并可以定义多值属性 |
|  | 配置从HR系统回收的用户属性及其映射关系 |
|  | 配置从HR回收属性的静态动作或动态动作 |
|  | 允许对回收操作的过程进行定义、监控及错误后可进行重试 |
|  | 支持批量操作功能，并支持预导入功能 |
|  | 支持用户查看所属所有应用账号操作 |
|  | 应用管理 | 具有应用系统的基本管理（增、删、改、查）功能 |
|  | 可灵活扩展应用的属性定义，并支持定义多值属性 |
|  | 根据应用需要，选择不同的组织机构树进行供应（提供功能截图并加盖原厂公章） |
|  | 根据应用需要，为应用配置同步的组织机构属性映射 |
|  | 根据应用需要，为应用配置同步的帐号属性映射 |
|  | 查询已供应给应用系统的组织机构 |
|  | 查询已供应给应用系统的应用账号 |
|  | 允许对供应操作的过程进行定义、监控及错误后可进行重试 |
|  | 账号管理 | 手动为用户/用户组分配应用账号 |
|  | 通过定义策略，自动分配应用账号 |
|  | 支持应用账号的孤立、采纳、启用、禁用、删除操作 |
|  | 允许一用户在一个应用中开通多账号的场景（提供功能截图并加盖原厂公章） |
|  | 具有应用账号的回收功能 |
|  | 可以批量开通/孤立/采纳/删除等操作，并能进行预处理 |
|  | 可以进行应用端和服务端的账号比对检查 |
|  | 允许对应用账号供应过程进行定义、监控及错误后可进行重试 |
|  | 支持云架构部署 |
|  | 支持docker等容器部署 |
|  | 支持云服务，如redis,RDS,SLB等 |
|  | 身份认证及访问管理 | 允许使用多种用户名登录(统一用户名/AD用户名/邮箱/手机号等) （提供功能截图并加盖原厂公章） |
|  | 支持双因素认证(例如：静态口令+Ukey / 短信验证码) |
|  | 用户自助修改统一用户名 |
|  | 多次认证错误后锁定统一用户 |
|  | 支持SAML协议，并同时可支持IDP和SP功能 |
|  | 多种集成方式，例如协议模式、代理模式、代填模式 |
|  | 支持JAVA/.Net/PHP应用的SSO集成 |
|  | 支持Oauth协议，可扩展微信登录 |
|  | 支持SharePoint、Domino等典型B/S应用的SSO |
|  | 支持扫码登录 |
|  | 支持PC和APP交互登录 |
|  | 支持多种认证方式融合 |
|  | 支持多证书体系的融合认证 |
|  | 支持桌面登录与APP交互登录 |
|  | 支持认证和单点登录风险预警 |
|  | 支持根据不同的风险基本自动提升认证级别 |
|  | 支持制定风险规则及风险策略 |
|  | 支持异地登录预警 |
|  | 支持IP地址异常预警 |
|  | 支持异常设备预警 |
|  | 支持主流的LDAP和数据库存储 |
|  | 支持云架构部署 |
|  | 支持docker等容器部署 |
|  | 支持云服务，如redis,RDS,SLB等 |
|  | 支持多种认证方式页面配置 |
|  | 支持认证链 |
|  | 支持国密加密方式 |
|  | 支持错误认证锁定机制 |
|  | 支持错误认证后解锁机制 |
|  | 支持认证鉴权机制 |
|  | 支持轻量级服务架构 |
|  | AD管理需求 | 回收AD组织机构（提供功能截图并加盖原厂公章） |
|  | 回收AD用户 |
|  | 给AD供应组织机构 |
|  | 给AD供应用户 |
|  | 对AD密码进行修改和供应 |
|  | 为AD用户分配/修改用户组及进行供应 |
|  | AD组管理 |
|  | AD组织机构管理 |
|  | Domino管理 | 回收Domino用户 |
|  | 给Domino供应用户 |
|  | 对Domino密码进行修改和供应 |
|  | SAP for ABAP管理 | 供应SAP for ABAP组织机构 |
|  | 回收SAP for ABAP用户 |
|  | 给SAP for ABAP供应用户 |
|  | 创建、删除、修改用户并供应至SAP for ABAP系统 |
|  | 对SAP for ABAP用户的禁用、启用状态修改及供应 |
|  | 提供SAP for ABAP指定生产密码和初始密码功能 |
|  | 提供SAP for ABAP组登录功能 |
|  | SAP for Java管理 | 供应SAP for Java组织机构 |
|  | 回收SAP for Java用户 |
|  | 给SAP for Java供应用户 |
|  | 创建、删除、修改用户并供应至SAP for Java系统 |
|  | 对SAP for Java用户的禁用、启用状态修改及供应 |
|  | 提供SAP for Java指定生产密码和初始密码功能 |
|  | 提供SAP for Java组登录功能 |
|  | 角色权限 | 基于RBAC进行角色权限管理 |
|  | 可对菜单权限、操作权限和数据权限进行管理 |
|  | 基于组织机构进行数据操作权限控制（提供功能截图并加盖原厂公章） |
|  | 基于用户组进行操作权限控制 |
|  | 基于目标系统进行操作权限控制 |
|  | 可对用户所属机构与管理机构的差异化进行数据权限控制 |
|  | 可对用户组进行权限管理 |
|  | 调度管理 | 提供调度作业/批处理引擎 |
|  | 支持手工及自动执行调度作业/批处理任务 |
|  | 灵活的参数配置功能，例如执行参数、执行周期等（提供功能截图并加盖原厂公章） |
|  | 提供调度作业/批处理运行检查功能，例如运行状态、结果、出错原因 |
|  | 审计及监控需求 | 所有操作均记录日志为前提；提供模板引擎，可灵活定制审计报告 |
|  | 审计报告可在线预览并以多种文件格式导出（提供功能截图并加盖原厂公章） |
|  | 提供用户类的审计 |
|  | 提供应用及账号类的审计 |
|  | 提供认证类的审计 |
|  | 提供集成应用访问情况的审计 |
|  | 自服务管理 | 用户通过自服务页面修改(授权允许其修改的)个人属性（提供功能截图并加盖原厂公章） |
|  | 用户查看其所拥有的应用访问权限和应用账号列表 |
|  | 用户自助修改统一用户名 |
|  | 自助修改统一用户密码 |
|  | 用户自注册统一用户名 |
|  | 自助找回密码 |
|  | 用户自服务页面 支持中英文 |
|  | 授权用户数 | 配置统一身份安全管理平台授权用户数3000个 |
|  | 实施接入应用 | **\*** PC端与蓝凌OA、Coremail、华为AC、深信服vpn PC端系统、盈高准入系统接入,提供证明材料并加盖统一身份认证系统原厂公章 |
|  | 移动端与蓝凌OA、Coremail、深信服vpn移动端系统接入 |