**设备详细技术参数**

1.下一代防火墙

|  |  |
| --- | --- |
| 技术指标 | 技术要求 |
| 品牌型号：安恒：DAS-NGFW890 |
| 产品资质 | 通过公安部检测并获得计算机信息系统安全专用产品销售许可证通过中国网络安全审查技术与认证中心检测并获得证书（增强级）通过IPv6 Ready Logo认证并获得证书具有中华人民共和国工业和信息化部颁发的《电信设备进网许可证》 |
| 规格要求 | 硬件架构：采用多核网络专用架构，使用64位MIPS多核处理器，非X86多核架构或ASIC架构产品规格：标准1U专用千兆硬件平台，内置交流双电源，硬盘≥500G网口数量：12\*GE电口，12\*SFP光口；支持千兆接口总数≥24个 |
| 性能要求 | 设备最大吞吐量≥8 Gbps，HTTP吞吐量≥4.7 Gbps，IPS吞吐量≥1 Gbps，AV吞吐量≥800 Mbps，IPSec VPN性能≥1.2 Gbps，最大并发连接数≥300万，每秒新建连接数≥10万，IPSec VPN隧道数≥1024，SSL VPN接入数≥1500 |
| 部署模式 | 支持路由、网桥、旁路、混合、虚拟线工作模式；部署模式切换无需重启设备 |
| 端口镜像 | 支持端口镜像功能，支持入流量、出流量和双向流量等维度镜像 |
| 接口 | 接口支持配置从属IP地址，每个接口要求支持至少200个second IP |
| 4G支持 | 支持4G接入，并可实现4G连接与有线链路之间的互为备份，支持的4G网卡必须包括华为E3372，支持在4G接口上运行IPSec VPN |
| DDNS | 支持DDNS功能，支持花生壳服务商的域名，将动态获取的IP地址映射为固定的域名 |
| NAT | 支持IPv4/v6双栈协议的源地址转换、目的地址转换、双向NAT、NAT44、NAT66、NAT46、NAT64等地址转换 |
| 路由支持 | 支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目标地址、用户、服务、应用、时间、域名的策略路由；ISP路由支持内置联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义 |
| DNS | 支持DNS透明代理，支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载 |
| 支持针对特殊域名使用指定DNS进行解析，支持域名定向解析 |
| 支持DNS解析动态缓存，缓存信息包括但不少于域名、IP、TTL和命中次数等。 |
| IPv6 | 支持IPv6/v4双栈，支持IPv6安全策略、包括审计策略、NAT策略、流量控制策略、会话控制策略、黑名单、白名单、认证策略等 |
| 支持IPv6策略路由、OSPFv3、静态路由、IPv6隧道，包括IPv6手工隧道、isatap、6to4等隧道模式、支持IPv6网络下的DHCPv6、DNSv6、SNMPv6、NTPv6、PPPoE等基础协议 |
| 支持IPv6入侵防御、病毒防护、Web防护、风险扫描、安全分析、资产发现、弱密码防护等安全功能 |
| VRF | 支持虚拟路由转发功能，使用VRF功能可以从系统层面隔离不同VRF组里的流量信息和路由信息，可作为MPLS组网里的MCE设备 |
| 不同VRF下的接口可以配置相同的IP地址 |
| 支持VRF静态路由 |
| 双机热备 | 支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，链路探测 |
| 访问控制 | 支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、日志记录、会话老化时间、终端过滤等高级访问控制功能 |
| 策略分析 | 提供智能策略分析功能，支持策略命中分析、隐藏策略分析、冗余策略分析、冲突策略分析、可合并策略分析、过期策略发现、空策略发现、策略宽松度分析，并在Web页面显示分析结果 |
| 入侵防御 | 系统定义超过8000+条主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、Web序列化、Webshell等主流防护类型。支持在线升级和手动升级 |
| 支持自定义IPS特征，至少支持IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等协议自定义入侵攻击特征；可拓展协议字段，设置数据包中的匹配内容；支持选择包含、等于、不等于、大于、正则匹配等匹配方式；可选择多种匹配条件，支持设置“与”和“或”的匹配顺序；支持设置检测方向，包括双向、客户端方向和服务端方向；支持自定义选择重要等级 |
| 支持日志聚合，可按照源IP、目的IP、防护规则和源目IP等维度进行聚合，方便管理员快速进行攻击事件统计和回溯 |
| 支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者syslog告警，不同告警规则可以发送给不同的用户 |
| 病毒防护 | 支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀，支持查杀邮件正文/附件、网页及下载文件中包含的病毒，支持400万余种病毒的查杀，并支持在线升级和手动升级病毒库 |
| 支持对最多20级的压缩文件进行解压查杀 |
| 端口扫描 | 支持针对IP、端口进行端口扫描，可选择立即执行或定期执行；支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能 |
| 基础防护 | 支持IPv4、IPv6双协议栈异常包攻击防御，攻击类型至少包含：Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP选项、IP Spoof、Jolt2等 |
| 至少支持telnet、ftp、imap、pop3、smtp、rlogin、http、oracle、mysql、postgres等常见协议的防暴力破解功能，针对每种协议可自定义检测时长、阈值和阻断时长 |
| 支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口；支持通过流量自学习获得服务器合法的外联行为，检测流量中的异常访问流量，实现自动拦截；学习时长可选择1小时、12小时、一天、一周等 |
| 资产安全分析 | 支持内网资产自动发现功能，开启后自动评估内网资产安全，无需人工干预。支持手动创建、导入导出资产信息 |
| 支持展示内网资产的风险级别、IP、用户、部门、操作系统、重要程度、受攻击总数、来源等内容。 |
| 支持数据下钻至单资产风险详情，可自动关联该资产所有安全信息，安全信息包括但不少于：入侵防御、威胁情报、WEB防护、病毒防护、防暴力破解、非法外联防护、弱密码防护、扫描攻击防御和行为模型等，支持以趋势图方式按时间展示各类安全事件的趋势，方便管理员快速了解资产安全状况，以便进行准确的安全防护 |
| 应用识别 | 应用特征不少于5000个，移动应用不少于450个 |
| 支持应用智能识别，有效识别P2P和迅雷行为，识别模式可选择严格、适中、宽松，支持排除扫描端口 |
| 支持智能识别模式和快速识别模式，在智能识别模式下应用引擎尽可能地用各种方式识别网络流量，在快速识别模式下应用引擎将关闭部分智能分析功能以提高性能 |
| 防私接路由 | 支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和阻断。 |
| 针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长。 |
| 认证 | 本地认证、Portal认证、Radius认证、LDAP认证、POP3认证、AD域单点登录、短信认证、微信公众号认证、APP认证、二维码认证、互联网钉钉认证、混合认证和免认证，其中微信公众号认证支持通过小程序获取手机号。 |
| 支持用户MAC感知，当用户MAC地址变更后，要求重新认证，避免冒名认证现象；支持伪Portal抑制技术，支持通过http302重定向或html-refresh方式抑制非正常的http或https的页面请求，从而保障系统稳定高效运行；支持基于https协议推送认证页面。 |
| VPN | 支持IPSec VPN、SSL VPN、Gre VPN，支持手机、平板电脑等移动终端VPN接入，功能标配，无需增加功能授权即可使用 |
| 支持标准IPsec VPN和快速IPsecVPN，标准IPsecVPN认证方式包括但不限于国密认证、数字证书和预共享密钥；同品牌设备快速IPsecVPN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IPsec VPN冷备份技术，指定VPN主备链路，当主链路存活时，备链路不接受不发送报文，避免主备链路同时收发包来回路径不一致导致业务中断的情况。 |
| 证书要求 | 具有国家信息安全测评信息安全服务资质证书（安全工程类三级）具有国家信息安全测评信息安全服务资质证书（风险评估二级）具有软件能力成熟度模型CMMI5认证具有知识产权管理体系认证证书 |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于硬件保修、系统升级等服务内容； |

2.数据库审计

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 品牌型号：美创DAS-G1010 |
| 授权数量 | 配置可管理数据库实例数量≥6 |
| 产品形态 | 1U、单电源、标配电口数量≥6个、内存≥8G、存储空间≥1T。 |
| 数据库类型 | 支持Oracle、SQL Server、MySQL、DB2、DM、Hive、Informix、Sybase、PostgreSQL、MariaDB、KingBase、GBase、hbase、优炫（UXDB）、greenplum、GaussDB（高斯）、tibero、MongoDB等数据库。 |
| 支持从网络流量中自动发现数据库信息，并添加到审计平台；支持自动扫描IP地址段，发现数据库信息，并可添加到审计平台。 |
| 部署管理 | 同时支持旁路镜像部署模式和探针部署模式； |
| 在旁路镜像模式下，通过TAP、SPAN等技术将网络流量映射到审计设备，对数据库流量进行审计和告警；支持VLAN、上下行链路、冗余链路环境的审计，支持多端口组管理。 |
| 在探针模式下，通过探针将数据库的所有操作传送到审计设备；探针支持自动推送安装。 |
| 支持探针性能的限制，防止对数据库性能产生影响。 |
| 提供集中化管理平台，基于Web的管理方式和SQL管理接口，B/S架构模式。 |
| 支持审计平台分级部署，对多台审计设备可进行统一管理、审计事件统一查询、策略统一下发、报表统一生成等功能。 |
| 加载数据库审计系统后，不需要改变现有应用程序和数据库的设计，无需改变应用程序代码，无需应用做二次开发，编写接口等。 |
| 审计功能 | 实现SQL语句的细粒度审计，并记录详细的用户行为信息，包括该语句执行的时间、机器名、用户名、IP地址、交换机端口、MAC地址、客户端程序名以及SQL语句、执行结果、执行时长、返回行数、结果集等信息，对数据库操作进行审计，可对查询，新增，修改，删除等行为进行监控。 |
| 支持按数据库进行双向审计、单向审计策略配置，可根据数据库定制审计力度，双向审计支持结果集展示。 |
| 支持按数据库进行白名单、黑名单审计策略配置，按客户端IP、应用程序、数据库用户配置黑白名单，过滤审计流量，可降低探针网络带宽压力，减小审计存储压力。 |
| 实现数据库登录操作的审计，并记录详细的成功登录行为和失败登录行为信息，能够识别暴力破解等非法登录行为。 |
| 支持三层审计，支持J2EE的B/S下的三层审计；支持中间件：开源的tomcat、jboss 、商业的weblogic、webshere等；数据库审计系统可以精确的识别操作人，可以精确的识别来自于B/S架构的浏览器终端信息；能精确识别到操作人和应用程序账户，可以与现实真人互相匹配。 |
| 支持Oralce、MySQL数据库本地审计；支持客户端SSH隧道代理访问数据库审计；支持本地命令行访问数据库审计。 |
| 支持复杂网络环境下重复包、乱序包审计。 |
| 事件处理 | 提供审计事件审阅和自动审阅，自动审阅的审计信息后续出现将不需要再行审阅；依赖于审计信息的访问规则的单键生成,依赖于审计信息的订阅规则的单键生成； |
| 支持审计查询结果下载，自定义设置下载字段，下载审计查询的结果。 |
| 支持审计事件FTP服务器自动备份功能，备份记录支持恢复到平台。 |
| SQL语句提供直译和意译的不同翻译引擎，从英文翻译成中文，增加易读性  |
| 内置大数据搜索引擎，支持模糊检索，10亿条以上的数据检索速度要求在秒级别实现。 |
| 告警策略 | 根据IP地址、机器名、时间、程序名，sql语句等精细组合对数据库敏感操作行为预设警报策略，并能够为特定的审计需求自定义审计警报规则。 |
| 提供多种安全响应措施，包括数据库记录、邮件报警、短信报警等。通过这些监控和防御措施，对招标方重要信息进行有效的监控、预防和保护。 |
| 模型分析策略：以操作语句为原型，根据获取的审计内容字段、表名称、条件字段、操作频率等条件设定分析策略。 |
| 对于首次出现的终端（IP）、人（用户名、账户），进行高级告警。 |
| 对于疑似威胁的操作记录，能够基于会话进行追踪溯源，根据人（用户名、账户）进行追溯，在同一界面展现跟其相关的从登录、访问到退出的全过程 |
| 根据不同的安全级别采用不同的响应方式，包括记录、告警。 |
| 告警方式包括：邮件、短信、SYSLOG。 |
| 安全告警必须支持基于订阅的模式，每个人可以订阅自己的安全告警事件，页面的安全告警事件必须区分开当前30分钟的安全告警事件和过去的安全事件以方便阅读，支持任意组合的规则订阅，实现人员的个性化订阅管理。 |
| 分析与报表 | 定期自动生成：日、周、月、年度综合报表； |
| 生成的综合性分析报表，包括但不限于：数据库风险、客户端风险、规则风险分析；客户端工具分析、账号使用情况分析、权限变更分析、认证管理分析、SQL错误分析、SQL平均执行时长、执行次数最多、最少的SQL语句、DDL、DML、DCL分析报表、各维度时间趋势分析等。 |
| 支持按时间、范围、报表模板自定义生成报表； |
| 支持下载法规性报表，如SOX法案、PCI报表、等级保护报表； |
| 综合报表展现形式具有多样性，如使用表格、柱状图、饼状图、折线图等多种方式进行展现分析； |
| 所有报表都支持下载；文档支持格式：包括WORD\HTML\PDF\EXCEL等； |
| 定期生成的报表可配置邮箱，定时收取最新生成的报表。 |
| 产品资质 | 具备国家版权局颁发的《计算机软件著作权登记证书》。 |
| 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》。 |
| 具备保密局颁发的《涉密信息系统产品检测证书》。 |
| 原厂商资质 | 原厂商具有ISO27001信息安全管理体系认证证书、ISO20000信息技术服务管理体系认证证书、ISO9001：2008质量管理体系认证证书。 |
| 原厂售后服务 | 要求项目经理具备项目经理和OCM证书；要求项目实施人员具备OCP和CISP证书。投标时需提供证书复印件加盖原厂商公章，并提供社保证明。 |
| 原厂商在宁波本地拥有分公司或服务机构，遇到产品自身问题时，可以提供2小时以内的上门服务。提供营业执照等相关证明材料原件复印件并加盖公章。 |
| 原厂质保服务 | 承诺中标公示期间提供设备原厂商针对此项目三年7\*24原厂质保服务函 |

3.日志审计

|  |
| --- |
| 品牌型号：宇视：NLI-2000 |
| 系统架构 | B/S架构，采用HTTPS方式远程安全管理，无需安装管理客户端 |
| 数据存储要求 | 支持各类非结构日志数据云端加密存储备份；系统内置云存储安全接入系统接口 |
| 监控功能 | 支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况 |
| 支持自定义配置实时监控的日志类型 |
| 支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警 |
| 支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况 |
| 报表分析功能 | 系统内置多种类报表模板 |
| 支持动态\静态（日报、周报、月报）两种系统生成方式 |
| 支持报告的邮件转发、生成提醒功能；支持多人邮件接收 |
| 支持自定义审计报告 |
| 支持导出html、Excel、PDF |
| 支持管理员自定义审计报表模板 |
| 查询分析功能 | 支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索； |
| 支持以日志类型、时间范围及条件字段快速检索过滤 |
| 支持高级检索以多条件组合查询方式，可以将每一个日志字段作为查询条件进行查询 |
| 支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件 |
| 支持查询模版创建、修改、删除功能 |
| 支持查询结果导出 |
| 支持海量日志数据高性能查询以及行为审计分析引擎 |
| 策略管理功能 | 支持内置关联分析策略，可设定用户在规定时间内连续多次输入错误口令产生告警或事件 |
| 支持自定义创建实时审计规则：根据日志字段为条件预设置分析策略 |
| 规则条件设定支持逻辑运算符与支持正则表达式 |
| 支持以告警页面、短信、邮件、SYSLOG、SNMP等各种方式呈现告警信息 |
| 数据管理功能 | 支持按日志属性、日志类型、时间范围等进行数据备份；  |
| 支持WEB界面备份及日志恢复导入工作 |
| 支持自动与手动两种备份归档方式 |
| 系统支持以FTP上传方式将归档文件存储到第三方存储系统中 |
| 系统配置功能 | 支持审计系统用户（组）管理（添加、修改、删除、停用、启用） |
| 支持资产管理，即所有采集日志源管理维护 |
| 支持密码长度、复杂度，密码猜测自动锁定账号以及系统超时设置安全策略 |
| 支持证书页面生成下载 |
| 支持系统配置备份恢复 |
| 支持时间同步页面配置 |
| 支持页面方式系统升级以及设备关闭、重启 |
| 支持从WEB界面查看网卡IP设置，修改静态路由设置等内容 |
| 支持安全页面（SSL）证书下载 |
| 系统自身安全 | 系统内置安全防火墙 |
| 支持控制访问审计主机范围 |
| 必需提供内部通讯检查机制，传输128加密 |
| 管理接口支持串口或电口的方式管理 |
| 管理界面与其他功能模块分离 |
| 日志数据安全 | 审计日志文件方式存储 |
| 审计日志加密导出审计系统 |
| 支持对所有审计管理员操作审计系统的动作进行审计 |
| 日志权限 | 审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明； |
| 支持日志类型、IP地址权限设置 |
| 支持页面功能模块权限设置 |
| 系统许可方式 | 授权永久许可方式,支持审计源数量100台 |
| 公司资质 | 制造厂商应具有良好的软件开发能力，确保系统软件的可靠稳定，获得过CMMI 5等级认证证书；为确保整个系统的安全，要求设备厂商具备关于网络及安全解决方案的安全测评报告 |

4.堡垒机

|  |  |
| --- | --- |
| 技术指标 | 技术要求 |
| 品牌型号：安恒：DAS-USM150 |
| 产品资质要求 | 通过公安部检测并获得计算机信息系统安全专用产品销售许可证（运维安全管理产品-增强级）通过中国网络安全审查技术与认证中心检测并获得证书（增强级） 通过国家网络与信息系统安全产品质量监督检验中心测评并获得信息技术产品安全分级评估证书（评估保障级3增强级）通过IPv6 Ready Logo认证并获得证书通过国家保密局检测并获得涉密信息系统产品检测证书 |
| 规格要求 | 软硬件一体化产品，1U、磁盘空间不少于1T、至少配备6个100/1000M自适应电口 |
| 性能要求 | 可管理设备数量≥100个，运维用户无限制单台堡垒机字符类并发会话≥100、图形类并发会话≥20 |
| 设备部署 | 设备采用旁路部署，不得影响业务环境；须支持HA主备模式，管理口和心跳口须支持多链路端口绑定功能，防止单网卡或单线故障 |
| 支持多台堡垒机异地备份部署，每台设备都能提供运维和审计服务，配置数据自动同步 |
| 支持集群部署模式，中心采用HA，节点可以横向扩展，实现统一登录入口、统一配置同步、审计日志集中查询、实时会话集中监控，以满足业务增长需求。 |
| 用户管理要求 | 用户角色 | 支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理 |
| 用户管理和用户策略 | 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 |
| 部门层级管理 | 支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据。 |
| 部门用户管理 | 每个部门可以管理本部门及下级部门的用户角色：部门管理员、运维管理员、审计管理员、运维员 |
| 部门资源管理 | 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 |
| 部门审计管理 | 每个部门的审计管理员可以管理本部门及下级部门的运维会话日志 |
| 身份认证要求 | 内置VPN | 产品内置VPN模块，无需与其他VPN设备联动，实现运维入口安全接入 |
| 与第三方认证对接 | 支持与AD、LDAP、RADIUS、吉大正元、北京CA认证系统联动登录堡垒机，[支持自动同步AD/LDAP用户](#_支持AD、LDAP、Radius等认证方式) |
| 短信口令认证对接 | 支持与get、post、soap发送方式的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、SendCloud联动 |
| 手机APP动态口令认证 | 支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令。 |
| 双因子认证 | 堡垒机须内嵌动态令牌和usbkey认证引擎，可同时使用动态令牌和USBkey |
| 密码存储 | 支持采用国密加密算法进行核心敏感数据加密存储 |
| 多种双因子认证同时使用 | 基于不同的用户设置不同的双因子认证模式，如user1用动态令牌、user2用USBkey、user3手机APP动态口令认证 |
| 多种认证组合使用 | 支持域认证与双因子认证结合使用，如同时使用AD/LDAP用户名+AD/LDAP密码+手机APP动态口令登录堡垒机、[同时使用AD/LDAP用户名+AD/LDAP密码+短信口令登录堡垒机](#_直接使用登录堡垒机的AD/LDAP用户及密码可以直接自动登录到服务器里_1) |
| 用户锁定 | 可设置用户密码错误达到一定次数后的锁定时长及登录失败次数的重置时间 |
| 用户密码策略设置 | 可以设置用户密码的长度、复杂度、相关度，其中相关度可以设置密码与用户名的关系，可以选择是否检查历史密码。并可支持密码过期前告警 |
| 认证窗口全局设置 | 支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口（ |
| 设备管理要求 | 支持的协议和应用 | 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具 |
| 主流数据库运维管理 | 支持DB2、oracle、mysql、sqlserver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 |
| IE代填 | IE/Chrom代填应用发布：HTTP/HTTPS协议的web设备，且可以直接代填账号和密码 |
| 混合云管理 | 可以通过socks5/http/ssh等代理协议连接管理异地云资源区中私有网络的云主机 |
| 分组管理 | 支持对设备进行按设备类型分组、按部门分组，支持设备批量导入/导出 |
| 登录模式 | 支持设备帐户和密码的自动登录、手工登录、二次自动登录模式 |
| 共享账户 | 支持设置共享账户，用于不同主机拥有相同账户名及密码的场景 |
| 自动收集和自动授权 | 支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权 |
| 设备密码管理 | 导出的设备信息文件加密存储，解密时须由2个管理员同时解密才能查看到设备信息文件内容 |
| 工单流程要求 | 申请工单 | 运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员。 |
| 审批工单 | 管理员对运维工单进行审核之后以邮件方式通知给运维人员；如果允许，则运维人员才可访问；否则就无法访问。 |
| 自动改密要求 | 自动改密 | 支持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能。 |
| 改密脚本 | 可以通过编写改密脚本的方式进行改密操作 |
| 改密保护机制 | 支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、改密后备份、密码文件加密；支持发送方式，包括邮件、FTP、SFTP等 |
| 密码容错机制 | 支持自动密码恢复、手工验证密码、密码强度控制等 |
| 运维方式要求 | 多种浏览器登录 | Web访问方式：至少支持使用IE、谷歌、火狐三种浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等运维客户端工具 |
| H5运维方式：支持ssh、telnet、rlogin、rdp、vnc协议的H5运维，无需本地运维客户端工具 |
| 连通性检测 | 支持对主机联通性、账号有效性进行周期性检测。并可设置是否开启检测连通性、有效性功能 |
| 数据库运维 | 支持通过堡垒机页面直接调用本地Windows系统里的plsql、sqlplus、toad、sqlwb、ssms、mysql.exe等数据库客户端工具 |
| 客户端工具登录 | 客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty等客户端工具登录堡垒机访问图形或字符设备，视图界面一致性、搜索能力 |
| SFTP/FTP的客户端登录 | 支持使用本地的winscp/flashFXP/SecureFX等客户端工具登录堡垒机访问SFTP/FTP设备 |
| SSH网关代理直连 | 支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备 |
| SSH -agent-forwarding | 可以使用SSH-agent-forwarding登录到ssh服务器，用于登录堡垒机和登录ssh主机使用相同私钥的场景 |
| SSH登录方式 | 可以使用密码或公钥的方式登录到SSH资产，并且可以发送运维用户信息、运维来源IP等环境变量到资产上 |
| 数据库代理直连 | 支持在mac电脑里使用navicat工具通过堡垒机登录mysql、oracle等数据库服务器 |
| 批量自动登录字符主机 | 支持批量登录字符设备功能：能自动生成SecurCRT/Xshell工具的批量登录文件，实现在工具中批量自动登录多台设备 |
| 批量登录 | 可一键批量登录不同协议的主机资产 |
| 快速运维 | 可记录最近运维的主机，用于快速对主机进行运维 |
| 域用户自动登录主机 | AD/LDAP环境，支持直接使用登录堡垒机的AD/LDAP用户及密码可以直接自动登录到服务器里 |
| 会话数量限制 | 可进行用户会话数量限制，允许自定义每个用户最多可以同时开启多少个会话 |
| 设备筛选 | 支持通过多个维度筛选待运维资产，可包括主机IP/主机名、操作系统、主机编码、主机组等。其中涉及到需要手动输入进行筛选的选项，需支持选择模糊搜索或精准搜索 |
| 审计日志要求 | 运维审计日志 | 支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容 |
| Zmodem传输审计 | 支持保存SSH的sz/rz命令（zmodem）传输的原始文件 |
| SFTP/FTP传输审计 | 支持保存SFTP/FTP传输的原始文件 |
| RDP粘贴板审计 | 支持保存RDP粘贴板（桌面之间复制-粘贴）传输的原始文件 |
| RDP磁盘映射审计 | 支持保存RDP磁盘映射传输的原始文件 |
| RDP文字记录 | 支持对RDP屏幕文字内容、标题窗口、键盘输入的记录和搜索定位 |
| SQL记录 | 支持审计主流数据库（如DB2、oracle、mysql、sql server）运维中的SQL语句，可进行关键信息定位查询 |
| 全文检索 | 支持全局搜索审计日志，无需区分图形/字符/文件/应用类型，只需通过关键信息直接搜索定位 |
| 审计规则 | 可针对审计操作进行规则设置，自定义用户与资产的审计关系，即可选择用户有权限审计指定设备的操作行为 |
| 日志数据归档 | 审计数据支持通过SFTP/FTP方式自动归档，并在页面中可以查询哪些数据是否归档。归档过程时，可以设置自动执行归档的时间以及归档传输的速度限制并可设置归档成功之后自动删除数据，归档后的数据可以用专用播放器离线查看 |
| 安全策略要求 | 运维规则策略 | 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、控制动作、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。 |
| 二次审批 | 对重要设备启用登录审核功能，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 |
| 命令审批 | 支持对重要命令进行审核：运维人员执行命令后，须等到管理员审批通过后才可执行成功 |
| 审批规则 | 对于审批操作，可以设置审批人及该审批人有权限审批的资产 |
| 自动运维任务 | 支持自动推送命令任务，如可自动备份交换机/路由器的配置信息、可自动执行周期任务；并将结果以邮件/FTP/SFTP的方式发送给相关管理员 |
| 运维空闲时间限制 | 支持运维空闲会话时间全局设置限制功能 |
| 报表统计要求 | 运维报表格式 | 内置丰富的报表统计模板，可点击柱状图、或曲线图进行数据钻取分析，且支持PDF、doc、html格式导出 |
| 运维报表内容 | 内置根据运维人员和组生成各种维度的分析报表，维度包含总为运维次数、时长、活动时长、会话起止时间、会话大小、命令数、上传下载文件数，分别从全局及平均值、最大值、最小值、单次运维、单个会话等角度提供非常有价值有意义的报表 |
| 自动发送报表 | 支持运维报表自动定期发送，提供一键导出符合等级保护、SOX法案要求的综合分析报告 |
| 系统管理要求 | 系统自审 | 支持自身审计，包括但不限于：系统状态检测、登录日志、用户配置日志、设备配置日志、授权配置日志、策略配置日志、运维访问日志、系统配置日志等 |
| 系统日志报表 | 支持系统日志报表统计功能，包括但不限于登录日志统计、配置日志统计、运维访问日志统计等，可以导出报表 |
| 系统语言 | 支持中文、英文、繁体中文，并可配置是否允许用户进行语言切换。 |
| LOGO设置 | 支持自定义WEB管理界面的LOGO |
| 告警输出 | 支持邮件/syslog方式输出告警日志 |
| SNMP输出 | 支持SNMP方式输出系统信息 |
| 排错功能 | 提供排错工具：ping、TCP端口检测、UDP端口检测、路由跟踪等 |
| API接口 | 需提供用户、资产、授权的增删改查等API接口，允许第三方平台调用堡垒机的API接口，实现用户、资产、权限自动同步到堡垒机，简化堡垒机配置工作量 |
| 与同品牌数据库审计联动 | 支持和同品牌数据库审计系统进行联动，将通过SSH/RDP等加密方式操作数据库的行为整合到数据库审计中，实现数据库行为的统一集中查询、展示、审计分析等 |
| 证书要求 | 具有国家信息安全测评信息安全服务资质证书（安全工程类三级） |
| 具有国家信息安全测评信息安全服务资质证书（风险评估二级） |
| 具有信息安全服务资质认证证书（信息安全风险评估一级） |
| 具有软件能力成熟度模型CMMI 5认证 |
| 售后服务 | 提供7\*24小时原厂商400支持热线；提供不少于三年质保服务，包含但不限于硬件保修、系统升级等服务内容； |

5.准入网关

|  |  |
| --- | --- |
| 指标项 | 招标技术要求 |
| 品牌型号：天融信：TSM-21128-TopNAC |
| 基本要求 | 采用专用硬件架构与专用安全操作系统（非Windows平台），硬件设备可以机架安装 |
| 1U机架式结构型。 |
| 6个1000BASE电口，2个SFP插槽，1T存储空间 配置单电源 默认电口具有一组BYPASS接口，冗余2个扩展槽位，最大用户数300 |
| 产品设计 | 信息安全设备、系统软件的开发、生产符合TL9000-HSV 标准 |
| 部署方式 | 系统部署简单，支持旁路或串联部署，串联部署采取透明网关准入模式时不依赖于交换机、路由器以及防火墙等设备，避免对已有网络进行较大规模的调整。 |
| 可靠性 | 支持双操作系统冷备，当常用系统出现故障可以使用备用系统恢复。 |
| 支持ByPass监控功能，用于对网络紧急情况的处理。 |
| 具备单机模式下的系统逃生工具，可添加维护交换机信息，在准入设备故障时进行自动或手动方式逃生 |
| 兼容性 | 客户端兼容：支持windows XP、32位及64位windows7/8/8.1/10/server2008操作系统。浏览器：浏览器插件兼容IE8及以上版本。 |
| 适应性 | 支持PC有线和智能终端无线认证，可与主流AC设备联动，实现智能终端无线准入，无需安装客户端。 |
| 准入模式 | 支持802.1X、Portal、透明网关、策略路由等多种准入模式选择，单设备情况下可进行混合准入模式应用 |
| 对于不同准入模式的介绍、部署拓扑、配置步骤等信息支持在管理界面中进行展示。 |
| 认证方式 | 提供Web认证方式，并可设置重定向页面URL地址。 |
| 提供客户端认证方式，采用用户名/密码认证，可与第三方AD域、LDAP服务器进行用户信息同步。 |
| 提供客户端认证及手机短信认证方式，客户端认证可与第三方AD域、LDAP服务器进行用户信息同步；手机短信认证可与短信服务器联动，在终端入网认证时下发验证码。 |
| 多要素绑定校验 | 支持信息绑定认证，可检查入网终端IP、终端MAC、用户名、交换机IP、交换机端口、终端硬件ID等多要素信息。 |
| 准入管理 | 支持同账户多在线管理，能够对同一用户同时刻允许使用终端数进行限制，处理方式包括：下线第一个、下线最后一个、不处理等 |
| 支持IP冲突管理，对入网终端与已在线终端IP冲突时提供处理方式，方式包括：下线已在线终端及不处理等 |
| 支持终端健康检查报告展示设置，可提供显示、不显示、失败时显示、成功时显示等多种展示方式 |
| 支持准入设备黑/白名单管理，可根据所应用的不同准入模式，设置黑/白名单终端IP、MAC、协议、端口、VLAN号等信息，以便针对该名单中设备进行入网控制。 |
| 支持动态终端IP分配功能，并可基于MAC绑定下发终端IP地址。 |
| 用户管理 | 支持认证用户管理，可创建组织结构并添加用户信息，信息包括登录名、姓名、密码、单位、电话、办公地址、邮箱、VLAN ID、ACL规则名等信息，可进行批量导入导出。 |
| 支持在线用户管理，界面展示入网用户信息，信息包括登录名、终端MAC、终端IP、准入模式、交换机IP、交换机端口、上线时间等，并可对在线用户进行强制下线及恢复操作。 |
| 入网健康检查 | 支持终端健康检查，系统默认检查项：系统时间检查；系统运行时长检查；Guest用户检查；AD域域名检查；Windows文件共享检查；Windows防火墙检查；必须/禁止运行进程检查；必须/禁止运行服务检查；必须/禁止安装软件检查；Windows桌面屏保检查；杀毒软件版本（小红伞、瑞星、金山毒霸、卡巴斯基、诺顿、360杀毒）检查项。 |
| 检查项策略对象之间可通过评分制的形式对终端的健康状况做最后的评估，根据预先配置好的阈值对终端入网请求作出判断。 |
| 可设置关键检查项与策略权重，并支持自定义修复向导与命令。 |
| 终端外设监控 | 支持终端接口外设监控，可对终端所有接口外设实施启停用控制，对USB设备添加USB硬件ID和设备信息，可设置例外项。 |
| 非法外联监控 | 支持终端非法外联监控，可判断通过http、telnet、ping三种方式检测主机违规外联行为，给予违规处理方式（不处理、重启、断网、提示），并信息提示。 |
| 入网资产管理 | 支持资产管理功能，可添加、修改、删除资产信息，资产类型包括：台式机、笔记本、打印机、IP电话机、服务器、工作站、手机等，并可对不同资产实施MAC免认证操作。 |
| 网络设备管理 | 支持网络设备管理，可添加、修改、删除网络设备，记录网络设备型号、IP地址、MAC地址、类型、使用人、登记时间等信息，并可点选查看设备名称、接口状态、接口类型、允许通过VLAN、是否开启MAC-VLAN、连接主机数等信息，支持设备接口802.1X启停用管理功能。 |
| 入网资产发现 | 支持资产发现功能，可扫描发现接入交换机连接设备信息，包括：终端IP、终端MAC、终端网卡供应商、终端VLAN、交换机端口、交换机IP、绑定用户等信息。 |
| 入网资产审批 | 支持未确认资产审批功能，记录入网终端操作系统、MAC地址、IP地址、计算机名、客户端/插件版本、终端ID等信息，提供确认或删除操作，终端确认后方可正常入网。 |
| 系统配置管理 | 支持系统配置保存、导入及导出，可进行恢复出厂设置、关机、重启操作。 |
| 证书要求 | 具有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》；设备生产厂家具有通信网络安全服务能力评定证书（风险评估二级）设备生产厂家具有中国网络安全审查技术与认证中心安全运维服务资质一级认证设备生产厂家具有CMMI成熟度认证五级证书 |

6. 机房环境控制系统

|  |  |  |
| --- | --- | --- |
| 序号 | 材料名称 | 规格型号 |
| 一、供配电系统 |
| 1 | 三相电量仪：品牌型号：约顿YD-BSQ305 | 1.可实现三相四线或其它任意线制的电压、电流等全部电参数的测量，RS485网络连接，支持MODBUS规约,超强电磁兼容能力、性能优越,指示灯指示工作状态：运行、电能脉冲、通讯发送、通讯接收;2.电压、电流信号经过离散化计算得到，计算值为有效值（RMS）;3.可以测量相电压、线电压、有功功率（W）、无功功率（Q）、和视在功率（S）、功率因数、频率；4.对电度量进行较为精确的计算，在一定程度上，可以提供给用户用为计费参考。5.绝缘及耐压：输入/输出/电源之间：≥20MΩ(DC500V)；2kV/min.2mA6.电磁兼容:符合IEC61000-4相关标准7.稳定性：温度影响：100ppm/℃8.长期稳定性：≤0.5%/年9.工作条件：温度：-15℃～55℃，湿度：20%～95% RH10.存储条件：温度：－40℃～80℃，湿度：10%～95% RH |
| 2 | 空开监测仪：品牌型号：约顿YD-MSV300 | 6路220V AC输入，监控6路配电开关（空气开关）的通、断状态  |
| 3 | 零地电压采集模块：品牌型号：约顿YD-IN304 | 1、采集单相电参量，包括电压、电流、功率、电能等多个电参量，信息全2、采用工业级芯片，内置看门狗，并具有完善的防雷抗干扰措施，保证可 靠性3、高隔离电压，电压电流输入信号采用微型精密互感器隔离，耐压达DC2500V4、35mm 标准DIN导轨安装，多种接线方式，方便现场安装布线  |
| 4 | 电缆温度检测单元：品牌型号：约顿YD-BM200 | RS485通讯 |
| 5 | 电缆温度传感器：品牌型号：约顿YD-TH01 | 无线测温探头 |
| 6 | 配电通讯软件：品牌型号：约顿NET300 | 　 |
| 二、UPS监控系统 |
| 1 | UPS接入：品牌型号：约顿Yeton-net300-UPS | 采集UPS的输入电压，输入电流，输出电压，输出电流，旁路相电压，旁路相电流，功率因素，电池电压，电池电流，系统频率，系统负载，电池后备时间等UPS通信协议所能提供的各项数据。 |
| 2 | UPS通讯软件：品牌型号：约顿NET300 | 　 |
| 三、普通空调系统 |
| 1 | 空调远程控制器：品牌型号：约顿YD-A/C | 1、监测普通空调运行状态，出风口及回风口温度等2、适用范围广：可适用市场上所有带红外遥控的空调机；3、节能性：可定时开关机、达到温度下限自动关机和温度自动调节功能，如客户调低空调的温度，空调控制器可自动恢复设定的温度；4、来电启动：空调来电1分钟内启动空调。 |
| 2 | 普通空调通讯软件：品牌型号：约顿NET300 | 　 |
| 四、漏水监测系统 |
| 1 | 区域漏水检测器：品牌型号：约顿YD-LD300 | 1、12V直流电源供电，区分正负极输入 |
| 2 | 漏水通讯软件：品牌型号：约顿NET300 | 　 |
| 五、温湿度监控系统 |
| 1 | 温湿度变送器：品牌型号：约顿YD-RS485 | 1、相对湿度：测量范围：0～99.9%RH2、温度：测量范围：-40～+80℃ |
| 2 | 温湿度通讯软件：品牌型号：约顿NET300 | 　 |
| 六、消防监测系统 |
| 1 | 烟感探测器：品牌型号：约顿YD-94II | 工作电压：DC9V~35V报警输出：常开/常闭可选 |
| 2 | 消防通讯软件：品牌型号：约顿NET300 | 　 |
| 七、门禁监控系统 |
| 1 | 单门门禁控制器：品牌型号：约顿YD-MDC200-A | 单门双向控制，2万张卡管理权限，10万条脱机存储记录，TCP/IP局域网广域网网络控制，可配置反潜回,多门互锁,多卡开门等扩展功能，含机箱电源  |
| 2 | 读卡器：国产 | 1、读卡距离：3—5CM2、读卡类型：EM/M1 |
| 3 | 出门按钮：国产 | 1、标准结构：铝合金面板，金属按钮2、适用类型：适用空心门框及埋入式电器盒使用3、面板处理：铝合金面板喷沙处理 |
| 4 | 卡：国产 | 1、薄卡 2、感应距离：3-12cm |
| 5 | 单门磁力锁：国产 | 1、适用于90度开的任何有框门2、带LED指示 (外装式) 3、抗拉力：230kg |
| 6 | 甲级防火门：国产 | 符合等保二级测评要求 |
| 7 | 门禁通讯软件：品牌型号：约顿NET300 | 符合等保二级测评要求 |
| 八、视频监控系统 |
| 1 | 网络摄像头：品牌型号：海康威视DS-2CD3325-I | 　 |
| 2 | 网络硬盘录像机：品牌型号：海康威视DS-7804N-K1/8P | 4路 |
| 3 | 专用硬盘：品牌：西部数据WD40PURX | 4T |
| 4 | 视频通讯软件：品牌型号：约顿NET300 | 　 |
| 九、系统配置 |
| 1 | 嵌入式一体化集中监控管理主机：品牌型号：约顿Yeton-III | 要求采用嵌入式linux操作系统，非PC操作系统；静态3D动环UI；传感器接口：8路RS485、4路RS232、8路开关量输入，3路模拟量输入，3路DO输出1路独立的RS232串口相机；传感器供电：主机能为传感器提供供电；2个独立的10/100M自适应以太网接口；安装方式：1U标准机架安装；宽工作供电电压：交流100~240V宽工作温度范围：-40°C ~ +85°C带外置独立看门狗支持ModbusTCP、SNMP v2.0、HTTP v1.1，系统配置灵活支持多种二次集成接口（Modbus JSON等）报警功能支持多方式选择、内容自定义、联动自定义、分组报警等，报警方式包含邮件、电话、现场语音、短信、彩信、声光、图像； 报警日志记录详细，含时间、说明、位置、方式、原因、接收人、现场图像等；功能要求：能实时检测市电、UPS、空调、漏水、温湿度、图像采集等设备的工作状态和各运行参数；在被盗、火灾、断电等异常状况下，完成关键数据采集、现场图像采集、报警信息发布、远程控制等操作；远程监控：WEB服务、移动终端远程监测和控制； |
| 十、报警系统 |
| 1 | 声光报警器：品牌型号：约顿YD-103 | 1、独立超高音喇叭设计，超大报警音量2、具备防拆功能，周期性进行自我功能状态检测，并向报警主机周期性进行性能状态汇报； |
| 2 | 微信报警系统：品牌型号：约顿YD-WX | 微信推送 |
| 3 | 一体化报警主机：品牌型号：约顿YD-ALARM | 参考品牌：约顿YD-ALARM、史图斯ST-YTH、英飞硕斯YF-202B1、要求采用嵌入式操作系统，非PC操作系统；2、以太网网口：1个10M/100M自适网口；3、TTS语音处理；4、GSM网络支持：1个SIM卡插槽，内置工业级GSM/GPRS模块5、固话网接口：1 个固话网电话线接口，物理接口：RJ-11插座6、开关量输入：4路光隔开关量输入；7、通信接口：1路标准RS232串口；8、音频接口：1路音频输入，1路音频输出；10、工作环境 温度：-10至60℃ ；湿度：10%至95%（无凝结）11、1U机架式安装12、为保证本分项货物的兼容性和集成性，投标人提供的货物必须集成移动客户端推送、短信、彩信、电话、语音、声光功能，不能采取分立方式。 |