# 技术需求书

重要性分为“★”、“#”和一般无标示指标。★代表最关键指标，不满足该指标项将导致投标被拒绝，#代表重要指标，无标识则表示一般指标项。

A,B,C,D类服务器为核心产品。

★为保证出口网络的高可靠和异构性，A类链路负载和B类链路负载不能为同一品牌；A类防火墙和B类防火墙不能为同一品牌。

★为保证出口网络的高可靠和联动性，A类防火墙和上网行为管理设备需为同一品牌。

★要求A,B,C,D类服务器为同一品牌；E类F类为同一品牌。

## 项目概述

现有人民日报社出口区设备陈旧，防火墙、交换机在性能、可靠性、数据吞吐能力上已无法满足日益增长的融媒体业务发展需求，并且设备老化严重，配件支持难度较大，故障维护时间较高。

## 采购产品一览表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备及软件名称** | | **数量** | **单位** |
| 1 | A类交换机 | | 3 | 台 |
| 2 | B类交换机 | | 4 | 台 |
| 3 | C类交换机 | | 3 | 台 |
| 4 | D类交换机 | | 2 | 台 |
| 5 | E类交换机 | | 10 | 台 |
| 6 | A类链路负载 | | 2 | 台 |
| 7 | B类链路负载 | | 3 | 台 |
| 8 | A类防火墙 | | 5 | 台 |
| 9 | 上网行为管理设备 | | 2 | 台 |
| 10 | B类防火墙 | | 5 | 台 |
| 11 | C类防火墙 | | 2 | 台 |
| 12 | 新一代威胁感知系统 | 流量采集 | 2 | 套 |
| 13 | 分析平台 | 1 | 套 |
| 14 | 漏扫设备 | | 1 | 台 |
| 15 | 日志搜索分析系统 | | 1 | 套 |
| 16 | 堡垒机 | | 2 | 台 |
| 17 | 集中管理平台 | | 1 | 套 |
| 18 | 智能网管软件 | | 1 | 套 |
| 19 | A类服务器 | | 5 | 台 |
| 20 | B类服务器 | | 14 | 台 |
| 21 | C类服务器 | | 6 | 台 |
| 22 | D类服务器 | | 9 | 台 |
| 23 | E类服务器 | | 1 | 台 |
| 24 | F类服务器 | | 1 | 台 |
| 25 | 服务器机柜 | | 3 | 台 |

## 产品清单及详细指标要求：

### A类交换机：3台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 硬件规格 | ★ | 交换容量≥2.5Tbps，包转发率≥450Mpps，支持24个万兆SFP+端口，2个40G QSFP+端口； |
| 二层功能 | 1 | 支持MAC地址≥32K，支持ARP表项≥20000  支持4K个VLAN，支持Guest VLAN、Voice VLAN，支持基于MAC/协议/IP子网/策略/端口的VLAN  支持1:1和N:1 VLAN交换功能 |
| 路由 | 2 | 支持静态路由、RIP V1/2、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6 |
| 堆叠 | 3 | 支持堆叠，主机堆叠数不小于6台。 |
| QOS | 4 | 支持WRR、DRR、SP、WRR＋SP、DRR+SP队列调度算法  支持报文的802.1p和DSCP优先级重新标记  支持L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源MAC地址、目的MAC地址、源IP地址、目的IP地址、端口、协议、VLAN的非法帧过滤功能 |
| 管理维护 | ★ | 支持以太网OAM（802.3ah 和 802.1ag），支持SNMPv1/v2c/v3，支持网管系统、支持WEB网管特性， 支持sFlow |
| 可靠性 | 5 | 支持G.8032标准环网协议 |
| 安全 | 6 | 支持DHCP Snooping，IP Source Guard，SAVI等安全特性  支持防ARP攻击、DOS攻击、ICMP防攻击、CPU防攻击  支持802.1ae提供安全的MAC层数据转发 |
| 实配 | ★ | 单台配置≥18个万兆多模光模块，≥6个万兆单模光模块，万兆堆叠线缆≥1根，可插拔冗余双电源，光模块支持数字诊断功能 |

### B类交换机：4台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 硬件规格 | ★ | 交换容量≥140Tbps，包转发性能≥29000Mpps，整机ARP表项≥200K，整机MAC表项≥512K ；整机主控引擎插槽≥2个，业务插槽≥5个, 电源≥4个，保证2块电源可以正常支撑设备运行； |
| 数据中心功能 | #1 | 可将多台物理设备虚拟化为1台逻辑设备，虚拟组内设备具备统一的二层及三层转发表项，统一的管理界面，并可实现跨设备链路聚合。 |
| ★ | 可将一台物理设备虚拟化为多台逻辑设备，各虚拟交换机间具备独立的转发表项及配置界面，各虚拟交换机的配置/重启互不影响。 |
| ★ | 满足L2-GRE国际标准MAC in IP数据封装技术（或同类其他技术），可实现跨广域网数据中心间二层数据通信，扩大虚拟机漂移范围。  满足OpenFlow协议，可实现核心网络向SDN平滑演进。 |
| 基础特性 | 7 | 满足Port based VLAN、Mac based VLAN、Guest VLAN、Restrict VLAN，满足多对一镜像,基于流的镜像，一对多镜像。满足SPAN、RSPAN远程镜像，满足VLAN的镜像；  满足IPv6静态路由、RIPng、OSPF v3、BGP4+ 等路由协议；  满足ICMP、ICMPv6、满足ND（neighbor discover）、手工配置（自动创建）本地地址、IPv6 Ping、IPv6 Tracert。满足手动隧道，自动隧道，ISATAP，IPv4 over IPv6；  满足MPLS转发，满足MPLS MIB(RFC1273,4265,4382)，满足跨域OPTION A/B/C三种模式，满足MPLS VPN/VPLS； |
| 配置要求 | ★ | 单台配置冗余1+1主控，≥4个交流电源模块；≥96个千兆电口，≥96个万兆光口，每台配置≥单模万兆模块48个，每台配置≥多模万兆模块48个，光模块支持数字诊断功能，每台配置万兆堆叠线缆≥4根。 |
| 资质 | 8 | 所投产品提供工信部入网证书 |

### C类交换机：3台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 整机规格 | ★ | 高度1U，交换容量≥2.5Tbps，包转发率≥1000Mpps，10GE光端口数量≥48个，40GE端口数量≥6个；内置电源开关，支持前后、后前风道； |
| 二层功能 | 9 | 支持4K VLAN;支持QinQ、Mux VLAN、Super VLAN;支持STP/RSTP/MSTP；支持端口隔离和端口组隔离； |
| 三层功能 | 10 | 支持静态路由、策略路由；  支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议；  支持RIPng、OSPFv3、ISISv6、\*BGP4+等IPv6动态路由协议；  支持BFD for OSPF，BGP，IS-IS，Static Route； |
| MPLS | 11 | 支持MPLS/BGP L3VPN； |
| 组播 | 12 | 支持IGMP Snooping V1,V2,V3；支持IGMP Proxy；支持PIM-SM,PIM-DM,PIM-SSM,双向PIM，MLDv1/v2； |
| 流量分析 | 13 | 支持netstream；支持sFlow； |
| DC特性 | 14 | 支持堆叠，最大支持堆叠交换机数量不少于6； |
| ★ | 支持Vxlan，支持VXLAN mapping,且支持BGP EVPN特性, 支持FCoE/DCB/DCBX； |
| DC管理 | 15 | 支持SNMP V1/V2/V3、Telnet、RMON、SSH;  支持通过命令行、中文图形化配置软件等方式进行配置和管理 |
| ★ | 支持端口镜像，流镜像、远程端口镜像（ERSPAN）；支持openflow协议 |
| 实配 | ★ | 每台配置≥2块40G多模光模块(850nm,300m)，≥48块万兆多模光模块(850nm,300m,LC) ，光模块支持数字诊断功能，万兆堆叠线缆≥2根，冗余电源，冗余风扇 |

### D类交换机：2台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 整机规格 | ★ | 交换容量≥590Gbps，包转发率≥250Mpps，≥48个10/100/1000Base-T以太网端口，≥4个SFP+光口；支持模块化可插拔双电源，支持1个扩展插槽，可扩展支持业务插卡 |
| 二层功能 | 16 | 支持64K MAC地址容量；支持4K个VLAN；  支持Guest VLAN、Voice VLAN；支持MUX VLAN功能或类似技术；  支持STP(IEEE 802.1d)，RSTP(IEEE 802.1w)和MSTP(IEEE 802.1s)协议； |
| 三层功能 | 17 | 路由表≥16000 ；  支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；  支持基于源IPv6地址、目的IPv6地址、四层端口、协议类型等ACL； |
| MPLS | 18 | 支持MPLS L3VPN、MPLS L2VPN(VPLS，VLL)、MPLS-TE； |
| 组播 | 19 | 三层组播组数≥2048 ；  支持VLAN内组播转发和组播多VLAN复制；  支持基于端口的组播流量统计；  支持IGMP v1/v2/v3、PIM-SM、PIM-DM、PIM-SSM |
| 安全功能 | 20 | 支持防止DOS、ARP攻击功能、ICMP防攻击；支持IP、MAC、端口、VLAN的组合绑定；支持黑洞MAC地址；支持CPU保护功能；支持CPU保护功能； |
| 堆叠 | 21 | 支持堆叠，主机堆叠数不小于6台； |
| 虚拟化 | 22 | 支持纵向虚拟化，作为纵向子节点零配置即插即用； |
| 管理维护 | 23 | 支持SNMPv1/v2/v3；支持网管系统、支持WEB网管特性；支持零配置部署； |
| SDN | ★ | 支持Openflow标准； |
| 实配 | ★ | 单台配置万兆多模光模块≥4个(850nm,300m,LC) ，光模块支持数字诊断功能，万兆堆叠线缆≥2根； |

### E类交换机：10台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 硬件规格 | **★** | 交换容量≥590Gbps，包转发率≥250Mpps；≥48个10/100/1000Mbps端口，≥4个SFP+光口,支持48GE+8XS 100%线速转发，可提供2个扩展槽； |
| **★** | 支持内置AC功能，实现有线无线一体化，最大可管理256个AP，同时支持集群功能，在主AC故障后可以切换到备AC，当主AC故障恢复后可切换回主AC； |
| 基本功能 | 24 | 设备MAC地址≥64K，ARP表项≥20K，FIB表项≥12K ；  支持RIP，OSPF，BGP，RIPng，OSPFv3，BGP4+；  支持IGMP v1/v2/v3，IGMP v1/v2/v3 Snooping，支持PIM-DM，PIM-SM，PIM-SSM，PIM for IPv6 ；  支持1对1、1对多、多对1和基于流的镜像；且支持RSPAN和ERSPAN； |
| 25 | 支持专门针对CPU的保护机制，能够针对发往CPU处理的各种报文进行流量控制和优先级处理，保护交换机在各种环境下稳定工作； |
| 26 | 支持专门基础网络保护机制，增强设备防攻击能力，即使在受到攻击的情况下，也能保护系统各种服务的正常运行，保持较低的CPU负载，从而保障整个网络的稳定运行； |
| 27 | 支持sFlow网络监测技术，可提供完整的第二层到第四层信息，可以适应超大网络流量环境下的流量分析，让用户详细、实时地分析网络传输流的性能、趋势和存在的问题； |
| 28 | 支持虚拟化功能，最多可将9台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤50ms； |
| 29 | 产品支持ITU-TG.8032国际公有环网协议ERPS,并且链路故障的收敛时间≤50ms； |
| 30 | 支持专门基础网络保护机制的NFPP功能，支持多种类型的防护，如ARP防护，当ARP速率超过攻击水线，对有攻击行为的用户进行隔离，保证设备和整网的安全稳定运行； |
| 管理特性 | 31 | 支持SNMPv1/v2C/v3、CLI(Telnet/Console)、RMON(1,2,3,9)、SSH、Syslog、NTP/SNTP、FTP、TFTP、Web； |
| 实配 | **★** | 单台配置≥1个万兆多模模块,≥1个万兆单模模块，光模块支持数字诊断功能，万兆堆叠线缆≥2根，配置冗余电源模块； |

### A类链路负载：2台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 硬件规格 | ★ | 支持千兆电口≥8个，千兆光口≥8个，万兆接口≥8个，配置≥8个光模块-SFP+-10G-多模模块，光模块支持数字诊断功能； |
| 32 | ≤2U机箱，多核非X86架构 ; 吞吐量≥20Gbps，并发会话数≥800万,支持内存≥32GB, 支持1路电口内置硬件Bypass模块； |
| ★ | 支持双硬盘插槽，硬盘容量≥1TB，硬盘支持可插拔更换，支持180天存储； |
| ★ | 支持1+1冗余电源，整机功耗低于300W； |
| 选路优化 | 33 | 支持静态路由、RIP(V1/V2)、RIPng、OSPFv2等多种路由协议； |
| 34 | 为保证在多条外网线路情况下带宽的合理分配使用，设备必须支持多链路负载均衡，负载均衡可基于带宽、负载等多种方式； |
| 35 | 支持线路过载保护功能，当某条外网线路拥塞时，自动将其流量切换到其他链路； |
| ★ | 冗余设备出现单点故障后可以平滑切换，可与互联设备进行联动确保实现业务链路故障的切换，ICMP丢包时间≤5s； |
| 36 | 支持正向DNS代理功能，可根据配置实现对不同外网线路的DNS服务器地址管理 |
| 37 | 支持应用路由功能，支持基于通讯、视频等应用进行路由选择 |
| 38 | 应用路由效果可通过图表呈现 |
| 39 | 支持智能DNS，无需内部服务器做任何修改情况下，为外网用户提供一个与该用户相同运营商的链路对内访问 |
| 上网行为管理及内容审计 | 40 | 行为审计策略提供系统配置模版;  HTTP流量管理策略支持时间对象设置，时间对象需精确至分钟级;  支持网站分类查询功能，可通过网址查询所属分类;  支持URL的黑白名单，支持基于用户/时间的URL过滤规则;  网址过滤策略，匹配阻断、放行策略后可根据需要先择是否记录日志;  HTTP访问行为阻塞后支持页面提示，避免内部用户反复尝试;  行为审计策略支持按用户查找功能;  支持URL过滤及审计，内置URL中文数据库，URL条目数≥2000万条;  要求所投产品URL数据库、应用分类库、地址库、内容审计特征库、QQ插件库支持至少10年免费升级，另外URL数据库和应用特征库支持远程HTTP自动升级; |
| 网络安全 | 41 | 支持状态检测防火墙功能，实现网络安全防护 |
| 42 | 支持防ping，防非法web登陆功能 |
| 43 | 支持防ARP欺骗、ARP静态绑定和停止学习功能，有效绑定ARP对应关系 |
| 44 | 支持基于IP地址段进行防攻击域配置，支持基于防攻击域进行防洪水攻击，收发速率限制，流量监控，黑白名单等策略。 |
| ★ | 支持SSL VPN，并提供≥300个免费SSL VPN接入授权 |
| ★ | 支持IPSec VPN，并提供≥3000路免费Ipsec VPN接入授权 |
| 45 | 支持WINDOWS、安卓、MAC、IOS操作系统SSLVPN客户端软件。 |
| 46 | SSLVPN可扩展支持UKEY功能。 |
| 47 | SSLVPN的WEB接入支持软键盘输入账号密码。 |
| 48 | ipsec vpn建立完成后能够自动生成拓扑图，便于监控各级单位设备在线状态。 |
| 49 | 支持防私接功能，可查看阻断的私接用户 |
| 50 | 防运营商检测，可以避免ISP ADSL线路封杀共享 |
| 设备管理监控 | 51 | CPU、内存使用率WEB界面可以展示;  支持HTTPS和HTTP的WEB方式管理;  支持网关、网桥等多种部署模式，灵活安装;  支持SNMPV2和V3版本，支持多TRAP接收主机配置; |

### B类链路负载：3台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 硬件规格 | ★ | 专用设备，非OEM，≤2U机架式设备，x86架构，千兆电口≥6个，万兆光口≥8个（配置≥8个万兆多模模块及2个万兆单模模块，光模块支持数字诊断功能），内存≥8GB，硬盘SSD容量≥240G |
| 性能 | ★ | 吞吐量≥20Gbps，并发会话数≥900万，四层每秒新建会话数≥30万，七层每秒新建会话数≥15万 |
| 部署要求 | 52 | 支持双机热备部署，设备之间同步会话信息；支持串接部署、旁路部署；支持三角传输模式； |
| ★ | 必须独立专业负载设备，非插卡式扩展的负载均衡设备 |
| ★ | 冗余设备出现单点故障后可以平滑切换，可与互联设备进行联动确保实现业务链路故障的切换，ICMP丢包时间≤5s。 |
| 动态路由 | ★ | 支持动态路由（ BGP、OSPF和RIP） |
| 多合一功能集成 | 53 | 单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权。 |
| 负载均衡算法 | 54 | 可以设置负载均衡策略,包括轮询、加权轮询、最小连接、加权最小连接、源地址哈希、最小延迟等策略。  内置国外域名地址库，国外域名不少于10万条，支持自动更新。可将访问国外域名的请求分发至指定线路，实现对国外域名访问的优化，提升用户体验。 |
| 上线保护 | 55 | 可以设置节点的最大请求速率增长幅度,包括:保持连接阈值、每秒新建链接阈值和每秒HTTP请求阈值 |
| 流量限制 | ★ | 可以支持客户访端的全面流量控制能力包括:最大并发数、最大带宽限制，可以设置上、下行的最大带宽限制，可以设置服务器连接池最大并发数。 |
| 会话保持机制 | 56 | 支持源IP、Cookie（insert/passive）、HTTP-Header、SSL Session ID、URL等多种会话保持机制 |
| Smart\_Rules脚本语言 | 57 | 可以支持基于LUA的高级脚本语言实现客户端请求/服务端响应双向控制 |
| TCP优化 | #2 | 可以提供TCP协议连接复用设置,包括连接池大小和老化时间可以提供TCP单边加速设置。 |
| SSL加速 | 58 | 可以支持软件的SSL卸载,支持客户端、服务器端双向数字证书认证,支持证书吊销列表联查,支持国密标准的证书 |
| IPv6 | ★ | 支持在不增加新域名NS记录和A记录的条件下解决IPv6改造过程中出现的天窗问题 |
| 59 | IPv6支持双栈模式，支持NAT46、NAT64、NAT66等协议转换;  IPv6改造方案支持多种模式和部署方案 |
| #3 | 支持常见的主动式健康检查功能，提供基于SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、RADIUS，ORACLE/MSSQL/MYSQL数据库等多种类型的探测判断机制。 |
| 60 | 支持TCP主动探测和TCP被动探测方式监测服务器节点健康状态 |
| 61 | 支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规HTTP应用可配置基于反映URL失效的HTTP响应状态码的观测判断机制，对于复杂应用可配置基于RST关闭连接和零窗口等异常TCP传输行为的观测判断机制。 |
| 业务交付优化 | ★ | 支持非对称式部署的TCP协议优化技术，提升远端用户访问应用服务的速度。无需在用户终端或应用服务器上安装任何插件和软件，不受操作系统类型、浏览器版本等兼容性因素限制，并且用户首次访问应用服务即可产生加速效果 |
| ★ | 支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的WebP或JPEG格式，优化加速效果 |
| ★ | 支持SSL卸载和加速功能，卸除服务器端的密集型运算任务，释放服务器计算资源，并提升SSL业务的处理速度。 |
| 链路繁 忙控制 | 62 | 支持HTTP缓存功能，利用内存Cache缓存用户频繁访问的web内容，降低后台服务器的负载压力,提升用户访问的响应速度。  支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。 |
| 服务器 繁忙控制 | 63 | 支持HTTP压缩功能，采用工业标准的GZIP或Deflate算法来压缩HTTP数据，从而减少传输数据量并降低带宽消耗，缩短客户端访问的下载等待时间。 |
| 64 | 支持TCP连接复用功能，利用HTTP连接池机制，将来自客户端的多个请求合并成一个连接发送到服务器，减少服务器端的工作负荷，并提升业务效率。 |
| 65 | 支持配置的服务器上线保护期，包括恢复时间和平滑上线时间 |
| 智能DNS功能 | 66 | 可以支持智能DNS解析策略,包括:轮询、加权轮询、静态就近性、顺序优先、返回所有IP、动态就近性、加权最小链接、加权最小流量、源/目地址哈希 |
| 67 | 支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。 |
| 服务器健康度调控 | 68 | 支持面向服务器健康度的弹性调控机制，可通过监控业务流中的TCP传输异常来衡量服务器节点的有效性，尝试对性能不足的服务器临时开启过载保护，动态调节服务器的负载。 |
| 安全防护 | 69 | 支持DOS/DDOS、SYN-Flood等防护策略、可以设置WEB服务器漏洞、网页编辑器漏洞、cms注入漏洞、远程文件包含漏洞、SQL注入漏洞、系统命令注入漏洞、文件上传漏洞、跨站脚本（XSS）漏洞、目录遍历漏洞、配置错误漏洞和WEBSHELL文件访问等防御策略 |
| 运维管理 | 70 | 内置智能告警系统, 支持E-mail、短信、SNMP Trap三种告警方式，管理员可基于业务安全所关注方面来选择告警触发事件与对应的告警方式，当业务网络环境中发生问题时（如服务器宕机、网络攻击、链路中断等故障场景），即会自动向管理员发送告警信息 |
| 第三方接口 | 71 | 提供基于Restful的API接口，提供接口清单 |

### A类防火墙：5台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 配置 | ★ | 整机吞吐量≥20Gb，应用层吞吐量≥12Gb，并发连接数≥800万，功能包含：传统FW、会话链接控制、入侵防御、僵尸网络检测、防病毒、实时漏洞检测、Web应用防护等功能； |
| 设备接口 | ★ | ≥4个千兆电口，≥12个万兆光口（配置≥12个光模块-SFP+-10G-多模模块，光模块支持数字诊断功能），并含2个高速USB2.0接口，1个RJ45串口 |
| 规格 | ★ | 设备≤2U，硬盘≥1T，支持硬件软件BYPASS，冗余电源 |
| 部署要求 | ★ | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式；  冗余设备出现单点故障后可以平滑切换，可与互联设备进行联动确保实现业务链路故障的切换，ICMP丢包时间≤5s。 |
| 路由支持 | 72 | 支持静态路由，ECMP等价路由；  支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；  支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能； |
| 基础功能 | 73 | 访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；  访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；  支持根据国家/地区来进行地域访问控制 |
| 内容安全 | 74 | 支持URL过滤和文件过滤功能，URL过滤支持GET，POST请求过滤和HTTPS网站过滤，文件过滤支持文件上传和下载过滤；  支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对HTTP、FTP协议内容检测与病毒查杀； |
| 入侵防护功能 | 75 | 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； |
| 76 | 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； |
| #4 | 支持系统服务器入侵防御、间谍软件入侵防御 |
| Web应用安全防护 | 77 | 设备具备独立的WEB应用防护识别库，特征总数在3500条以上； |
| 78 | 支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞； |
| 79 | 支持对网站黑链进行检测； |
| #5 | 支持Windows和Linux系统下网页防篡改功能，防篡改支持网站登录后台和FTP登录后台防护，管理员支持IP认证和邮件认证。 |
| 高级威胁 | 80 | 支持安全日志进行分析，识别持续性攻击、黑链、高危僵尸病毒等高级威胁并通过微信进行预警； |
| 僵尸主机检测 | 81 | 设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在50万条以上； |
| #6 | 支持木马远控防护、勒索软件通信防护、恶意链接防护、异常流量检测。 |
| 安全集中管理 | 82 | 支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能；  支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计；  双机支持A/S，A/A方式部署； |
| 系统配置管理 | 83 | 支持配置同步，会话同步和用户状态同步；  支持双机心跳线冗余；  支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式； |
| 配置 | ★ | ≥5年 防病毒升级和维护服务；  ≥5年 入侵防护升级和维护服务；  ≥5年 Web应用防护升级和维护服务；  ≥5年 僵尸网络检测升级和维护服务；  ≥5年 实时漏洞防护升级和维护服务； |

### 上网行为管理设备：2台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 通用 | ★ | 支持带宽≥2Gb，用户规模≥2万 |
| 设备接口 | ★ | ≥4个千兆电口，4个千兆光口，8个万兆光口，1个RJ45串口，配置≥8个万兆多模光口及2个万兆单模模块，光模块支持数字诊断功能 |
| 硬件规格 | ★ | 设备≤2U，硬盘≥2TB，冗余电源，支持硬件软件BYPASS |
| 多主模式 | #7 | 支持两台及两台以上设备同时做主机的部署模式； |
| 部署要求 | ★ | 冗余设备出现单点故障后可以平滑切换，可与互联设备进行联动确保实现业务链路故障的切换，ICMP丢包时间≤5s。 |
| 管理员权限分配 | 84 | 支持细致的管理员权限划分，包括对不同用户组的管理权限、对各种主要功能界面的配置和查看权限； |
| 告警管理 | 85 | 支持多种事件进行邮件告警，包括攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等； |
| Web访问质量监测 | #8 | 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，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向web访问质量检测。 |
| 首页可视化分析展示 | 86 | 支持首页分析显示接入用户人数、终端类型、认证方式；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况； |
| 多种认证方式 | 87 | 支持多种认证方式，包括本地用户名密码、第三方服务器、短信认证、微信认证、二维码认证等 |
| 无流量注销 | ★ | 支持按不同身份设置不同的无流量注销时间，如：  a) 内部员工30天。30天内有流量自动顺延30天  b) 其他接入用户7天，7天内有流量自动顺延7天  c) 访客每天8小时，超过后自动下线，不可顺延 |
| 用户数限额 | 88 | 用户限额策略里的在线用户数限制，超限后，支持能自动踢掉前面的用户 |
| 会议室场景 | ★ | 支持会议室场景的认证通过扫描二维码方式认证，扫码后需录入个人信息。 |
| 共享接入管理（防共享） | 89 | 设备能够发现私接路由（或者共享软件等）共享网络的行为： 1.支持自定义配置终端数量和冻结时间，和添加信任列表； 2.支持显示以IP或用户名的维度统计一段时间内的趋势图。 3.支持例外排除功能：如指定例外条件1台PC，2个终端。当PC或终端数超过例外条件才会被判定为共享。 |
| 应用识别规则库 | #9 | 设备内置应用识别规则库，支持不少于6000条应用规则数，支持不少于2800种以上的应用，不少于1000种移动应用，并保持每两个星期更新一次，保证应用识别的准确率。 |
| SSL加密内容审计和过滤 | 90 | 针对SSL加密的网站、论坛发帖、web邮箱的内容进行关键字过滤和内容审计； |
| 应用审计 | 91 | 1、支持记录QQ、TIM、微信、MSN等IM聊天行为和聊天内容； 2、支持移动APP（IOS和android）审计（如论坛类、微博类、新闻评论类等） |
| 加密证书自动分发 | #10 | 审计SSL网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台PC单独安装证书的问题。 |
| 上网流速提醒 | 92 | 用户指定应用上网流速超过预设阈值后，网关自动提醒该用户； |
| P2P智能流控 | 93 | 支持通过抑制P2P的上行流量，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； |
| 流控黑名单 | #11 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中。 |
| 时间控制 | 94 | 支持基于时间段的带宽划分与分配策略； 支持按日期设置流控策略，比如针对节假日设置不同流控策略； |
| 网络整体状况报表 | 95 | 从带宽健康分析、工作效率分析、离职风险分析、合规性分析四个大块对网络整体状况进行说明 |
| 搜索中心 | 96 | 基于时间、用户/组、终端类型、位置、日志类型等条件下的关键字检索定位功能；必须支持对日志中OFFICE等附件正文内容关键字的检索； |
| 支持与多种网安日志平台对接 | 97 | 内置多套日志模板与其他网安日志平台对接，至少支持以下平台：派博、任子行、网博、云辰、烽火、中新软件、兆物、新网程、美亚柏科、爱思等。 |
| 配置 | ★ | 配置≥5年免费特征库升级服务 |

### B类防火墙：5台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 配置要求 | ★ | 实配：千兆电口≥16，万兆光口≥12，配置≥12个光模块-SFP+-10G-多模模块，光模块支持数字诊断功能，40GE接口（含模块）≥2，SSL VPN并发数≥100，虚拟防火墙数量≥500，配置双电源；配置≥240G内置硬盘（或存储容量≥240G的服务器）做日志存储 ；  ≥5年免费防病毒升级服务；  ≥5年免费入侵防护升级服务；  ≥5年免费URL升级服务。 |
| 性能要求 | ★ | 吞吐量≥30Gbps，最大并发连接数≥750万，每秒新建连接数≥20万； |
| 硬件要求 | 98 | 支持SSD硬盘扩展，进行日志存储和安全分析 |
| 电源要求 | 99 | 支持交流、直流双电源 |
| 流量采集 | 100 | 为了有效掌握当前网络的使用情况，及时发现网络中的异常行为，具备采集网络流量的网络层、传输层和应用层信息。 |
| 部署要求 | ★ | 冗余设备出现单点故障后可以平滑切换，可与互联设备进行联动确保实现业务链路故障的切换，ICMP丢包时间≤5s。 |
| 策略管控 | 101 | 能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、VLANID、内容安全统一界面进行安全策略配置 |
| 路由功能 | 102 | 支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议 |
| 协议识别 | 103 | 可识别应用层协议数量≥5000种；支持识别国标SIP协议及主流安防厂家的私有协议 |
| 数据安全 | 104 | 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配 |
| 加密流量安全防护 | 105 | 支持对HTTPS，POP3S，SMTPS,IMAPS加密流量代理解密后，并进行内容过滤，审计，安全防护;  支持基于URL分类的精细化解密，提高解密性能;  支持恶意C&C流量监测; |
| 集中管理及易用性 | 106 | 支持防火墙向云管理平台自动注册，云管理平台对防火墙进行统一的管理及运维）；开放RESTCONF，NETCONF等北向接口，对接第三方的管理平台。 |
| 沙箱联动 | 107 | 支持与本地沙箱、云沙箱进行联动，实现APT等未知威胁检测与防御 |
| 多出口智能选路 | ★ | 可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式 |
| 智能威胁防御 | 108 | 具备基于AI技术检测DGA/ECA等APT攻击的威胁防御能力 |

### C类防火墙：2台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 设备性能 | ★ | 整机吞吐量≥5Gb，应用层吞吐量≥700M，并发连接数≥180万，x86架构，功能包含传统FW、会话链接控制、入侵防御、VPN、僵尸网络检测、防病毒、实时漏洞检测、Web应用防护等功能； |
| 设备接口 | ★ | 标准1U架构≥4个千兆电口，≥4个千兆光口（含满配多模千兆模块，光模块支持数字诊断功能），1个RJ45串口 |
| 部署要求 | 109 | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式； |
| 路由支持 | 110 | 支持静态路由，ECMP等价路由；  支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；  支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能； |
| 基础功能 | 111 | 访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；  访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；  支持根据国家/地区来进行地域访问控制； |
| 入侵防护功能 | 112 | 设备具备独立的入侵防护漏洞规则特征库，特征总数在7000条以上； |
| 113 | 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； |
| 114 | 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间； |
| 115 | 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； |
| #12 | 支持系统服务器入侵防御、间谍软件入侵防御。 |
| 高级威胁 | 116 | 支持安全日志进行分析，识别持续性攻击、黑链、高危僵尸病毒等高级威胁并通过微信进行预警； |
| 僵尸主机检测 | 117 | 设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数不少于50万条； |
| #13 | 支持木马远控防护、勒索软件通信防护、恶意链接防护、异常流量检测。 |
| 配置 | ★ | ≥5年免费防病毒升级服务；  ≥5年免费入侵防护升级服务；  ≥5年免费Web应用防护升级服务；  ≥5年免费僵尸网络检测升级服务；  ≥5年免费实时漏洞防护升级服务；  ≥5年免费VPN升级和维护服务； |

### 新一代威胁感知系统：2套流量采集+1套分析平台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 流量采集硬件规格 | ★ | CPU≥2颗，主频≥2.20GHz​，内存≥64G；电源：支持冗余电源；存储：≥4TB；接口：2×1GE千兆电口（管理口），2×1GE千兆电口（监听口）；2×10GE万兆光口（监听口）；并发会话：≥700万；新建会话：≥8万；流量吞吐：≥8Gbps |
| 流量采集 | 118 | 支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs等；支持自定义协议，可自定义私有协议 |
| 威胁发现 | 119 | 攻击结果：威胁检测告警能够直接体现攻击结果即企图、成功、失陷 |
| 120 | 支持基于流量实时IOC匹配功能，设备具备主流的IOC，情报总量50+万条 |
| ★ | 支持旁路IP阻断、域名阻断及重定向 |
| 联动功能 | #14 | 支持与分析平台、文件威胁鉴定器、Hadoop平台（kafka）、syslog服务器等联动 |
| ★ | 支持与现有终端安全软件联动。 |
| 文件处理 | 121 | 支持服务器威胁检测、支持发现恶意修改后缀的行为 |
| #15 | 支持云查杀引擎，不少于50亿条样本库大规模覆盖文件，快速返回判定结果，节省分析资源 |
| 122 | 支持文件缓冲池机制，在对于周期性重复验证时能够快速匹配已有结果 |
| 漏洞检测 | #16 | 支持检测文件运行期间漏洞利用行为，并支持第三方权威漏洞库信息共享 |
| 动态检测 | 123 | 可记录文件运行期间的注册表行为、文件行为、网络行为等所有行为记录，并可将详细的文件运行行为以报告形式提供 |
| 124 | 支持AES256、SM4数据传输加密，确保数据传输的安全性 |
| 125 | 支持灵活设置动态检测策略，包含全过动态、全不过动态和基于静态检测结果选择性过动态等策略配置 |
| 分析平台硬件规格 | ★ | CPU≥2颗，主频≥2.20GHz​，硬盘≥48T；接口≥4×1GE千兆电口 |
| 威胁分析 | 126 | 能够存储所有采集还原后的关键流量数据 |
| #17 | 支持基于威胁情报的威胁检测，检测类型包含APT事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报 |
| 127 | 支持对告警从多维度进行分析展示，维度包含：威胁情报、WEB攻击、邮件攻击、恶意软件、天擎、沙箱、攻击链（侦察、入侵、命令控制、横向渗透、数据外泄、痕迹清理） |
| 128 | 能够对告警进行深层次分析，分析内容包含：基本信息、主机详情、威胁情报详情、投递的恶意样本、在主机上运行的恶意样本、外联C&C服务器域名、C&C服务器会话记录、C&C服务器传送文件、受到的攻击等 |
| 129 | 能够对告警进行处置，可设置不同状态对告警进行跟踪 |
| 场景化分析 | 130 | 可基于机器学习和行为模型进行未知威胁和异常行为的检测，可检测异常行为包含：业务资产主动外连、HTTP代理、SOCKS代理、异常DNS服务器、DNS Tunnel、reGeorg Tunnel、DGA域名、异地账号登录、暴力破解、明文密码泄露、弱口令监测、敏感关键词邮件、敏感后缀邮件。 |
| 131 | 业务资产主动外连，检测行为特征包含：外连IP、外连IP归属、服务商、外连流量大小 |
| ★ | DGA域名发现，通过结合机器学习技术发现动态恶意域名，检测行为特征包含包含请求域名以及检测的准确率 |
| 132 | HTTP、SOCKS代理发现，检测行为特征包含：代理IP、代理端口、代理次数 |
| 133 | reGeorg Tunnel发现，检测行为特征包含：tunnel地址、关联图、操作命令、目标IP |
| 134 | 异地账号登录，检测行为特征包含：登录IP归属、账号、登录资产IP、使用协议、登录次数、登录成功率 |
| 135 | 暴力破解，检测行为特征包含：登录IP归属、使用协议、爆破次数、爆破成功与否 |
| 136 | 敏感关键词邮件，不仅支持自定义关键词发现恶意邮件还支持邮件白名单，检测行为特征包含：发件人、收件人、关键词、邮件主题、抄送、附件文件名、邮件正文 |
| 调查分析 | ★ | 威胁事件的追踪溯源分析能力，可基于事件告警进行调查分析，对攻击过程进行可视化展现，可展示命中威胁情报的内部主机之间的连接行为，能输出完整的基于时间序列和攻击链的事件报告，事件报告支持word格式导出 |
| #18 | 可对日志的关键字段进行追加搜索，从上一次的搜索结果中重新按照新的规则搜索日志 |
| 137 | 流量日志至少包含异常报文、域名解析、文件传输、邮件行为、Web访问、登录动作、FTP控制通道、数据库操作、LDAP行为、SSL加密协商等流量行为日志，并可按照以上应用协议的各个关键字段搜索日志 |
| 138 | 流量日志记录至少包含以下字段：时间、IP、MAC、IP地理位置、端口、域名、HTTP头信息、SQL语句、邮件收件人和发件人、文件名、文件MD5、应用层payload前100字节、协议 |
| 管理功能 | 139 | 可以搜索文件访问行为，并展示还原流量中文件的MD5和文件名；  报表提供快速报表和任务报表；  支持对日志进行导出备份以及导入恢复；  支持运营场景切换，提供默认的2个告警展示场景； |
| 部署功能 | 140 | 支持二级级联部署，下级分析平台向上级分析平台发送告警和相关信息，在上级分析平台上进行汇总展示  可以和终端安全管理系统联动，实现恶意文件的查杀、被感染主机的网络隔离（如可以对单个告警记录中的源IP进行网络隔离操作，对被告警的邮件附件进行查杀） |
| 可视化展示 | 141 | 支持展示网络风险指数、攻击三维地图展示、告警统计、受害主机统计、威胁检测统计、APT事件统计、攻击回溯、异常行为TOP5统计、攻击源国家TOP5统计、网络流量展示等内容 |
| 产品扩展 | 142 | 应对不同攻击，不影响原有网络架构的情况下分析平台可以接入文件威胁鉴定引擎数据，对文件样本进行检测分析，并在统一分析平台展现分析结果。 |
| 安全服务 | #19 | 支持与云端安全运营中心联动。设备能连接互联网时，安全专家在云端分析并撰写威胁分析报告下发到设备上共用户查阅；设备离线时，可将关键数据离线导出上传到云端安全运营中心，安全专家进行分析撰写威胁分析报告。 |

### 漏扫设备 1台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 设备 | ★ | 自主研发，标准机架式硬件，1U，含交流单电源模块，1个RJ45串口，1个GE管理口，≥6个10M/100M/1000M自适应以太网电口扫描口，≥1个接口扩展槽位（4GE/4SFP/8GE/8SFP）。 |
| 性能 | ★ | 最大并发任务数≥10个。并发扫描数≥60个IP地址，支持多路扫描。提供无限个扫描IP授权。最大扫描速度≥800 ip/h。 |
| 功能 | 143 | 支持检测的漏洞数≥50000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准。 |
| 144 | 支持IPv4和IPv6环境的部署和扫描。 |
| 145 | 同时支持远程扫描和采用SMB、SSH、RDP、Telnet等协议对Windows、Linux等系统进行登录扫描。 |
| 146 | 内置不同的漏洞模板针对Unix、Windows操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；支持自动模板匹配技术。 |
| 147 | 产品应支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息。 |
| 148 | 提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。 |
| ★ | 支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统。 |
| 150 | 支持专门针对DNS服务的安全漏洞检测，包括DNS投毒等漏洞检测能力；支持“幽灵木马”检测； |
| 151 | 支持针对大数据组件框架的漏洞检测。 |
| 152 | 支持扫描主流虚拟机管理系统的安全漏洞，如：VMWareESX/ESXi，要求能够扫描大于等于300条相关漏洞 |
| 153 | 支持Oracle、MySQL、MS SQL、DB2、Sybase数据库漏洞检查 |
| 154 | 支持智能端口挖掘，可以智能发现非默认端口启动的服务 |
| 155 | 产品支持对系统漏洞扫描、web漏洞、配置合规进行检查和综合分析，可输出同时包含漏洞扫描和配置核查结果的报表。 |
| 156 | 具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。 |
| 157 | 支持断点续扫，可对已完成的扫描任务中没有被覆盖到的目标重新下发扫描任务 |
| 158 | 支持复用已有任务配置用于新的扫描任务。 |
| 159 | 支持在线报表，在线查看展示各节点和主机资产风险分布、漏洞分布、配置合规和脆弱账号信息，在线查看设备风险详情。 |
| 160 | 报表能提供针对不同角色的默认模板，离线报告支持HTML、WORD、EXCEL、PDF等格式，报告可以直接下载或自动通过邮件直接发送给相应管理人员 |
| 161 | 支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态 |
| 162 | 提供备份恢复机制，能够对扫描结果、扫描模板、参数集等配置文件进行导出和导入操作；能够对系统创建还原点对系统进行备份和还原。 |
| 配置 | ★ | 配置≥5年免费特征库升级服务 |

### 日志搜索分析系统 1套

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 配置 | ★ | 核心引擎完全自主研发，非OEM产品。软件授权不限制接入日志源节点数；授权支持每日新增日志量25GB。 |
| 功能 | ★ | 数据源包含但不限于应用数据；数据库数据；系统数据；设备类数据 |
| 163 | 提供IT基础安全数据分析能力包括：从发现安全风险到定制安全策略，监控告警，从而提供整体分析视图、告警、报告的功能。 |
| 164 | 提供网络安全巡检报告，可以多维度提供内网安全设备巡检报告，包括但不限于按照时间维度，按照设备维度，按照操作维度等。 |
| 165 | 所有的解析功能，必须在Web界面完成，不得编译源代码、提交版本等方式完成，需要极其精简的方式完成数据解析工作，具有解析过程效率的统计。 |
| 166 | 客户端具有在线维护能力，可以实现在线升级、启动、停止、重启能力，具有数据压缩、加密、限速传输功能，支持设置客户端对服务器资源使用限制的能力；具有数据备份功能，能够将客户端的数据备份到服务器上，备份必须支持压缩，删除数据源等策略。 |
| 167 | 支持趋势图，可以通过拖拉拽的方式生成趋势图 |
| 168 | 要求有数据生命周期管理功能，能够对索引数据每天进行备份，恢复，且完全通过WEB界面配置操作完成。 |
| 169 | 平台提供自监控功能，支持查看整个系统及各个模块的运行状态，支持在线扩容，升级版本等功能 |
| 169 | 数据分组功能，要求对数据能够根据特定标识进行分组，以上操作全部通过WEB界面完成。 |
| #20 | 日志解析可通过正则自动学习生成，通过鼠标点选和划动拖拽的方式，由系统自动学习生成可用正则表达式 |
| 170 | 索引配置功能，要求能够根据索引保留时间和切分时间配置索引库信息，并能够通过特定标识将默认索引库数据路由到此索引中，用以应对数据量大的时候的提高系统性能，以上操作要求全部通过WEB端完成。 |
| 171 | 必须支持可分析的搜索脚本语言功能，完成各种复杂分析场景的需求，支持按照特定参数占比性分析、业务趋势变化分析，环比分析、同比分析等 |
| 172 | 支持全文检索、短语(多个词中间空格)搜索、字段过滤、逻辑运算搜索、数值范围搜索(数值比较运算，如>,<,<=,>=等)、通配符搜索、简单正则表达式； |
| 173 | 具有基于角色权限控制的功能，能实现对系统功能访问控制和数据访问权限控制 |
| 配置 | ★ | 配置≥5年免费产品升级服务 |
| ★ | 日志专用设备,配置CPU≥2 ，主频≥2.2GHz 核数≥10core；内存≥2条，单条≥32GB DDR3；SSD≥2，单SSD盘≥480GB ；SATA硬盘≥10，SATA硬盘容量≥3.84TB；≥1GB Raid缓存；≥2\*1Gb，≥2\*10Gb（含2块多模万兆模块，光模块支持数字诊断功能），冗余电源，5年免费质保 |

### 堡垒机 2台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 配置 | ★ | 系统以软硬件一体方式提供，硬件采用高性能服务器（不接受工控机），2U标准机架；千兆网络接口≥2个，硬盘容量≥2T\*2；支持≥100个图形并发访问，≥100用户并发访问，≥500个字符并发访问，配置管理大于等于500台目标设备许可。 |
| 兼容性 | 174 | 支持使用ie、google、360浏览器、火狐、猎豹、safari等常见浏览器实现所有功能； |
| 认证 | 175 | 支持静态密码、AD、Radius、证书认证、短信认证等多种登录认证方式，并且支持自定义二次认证登录；内置TOTP方式的动态双因素认证，用户不需要额外部署认证服务器；内置手机令牌认证，用户可以直接使用andriod、ios上的令牌APP产生的动态码，直接登录堡垒机；支持AD用户自动同步功能，可自定义用户同步的范围，支持按照AD安全组同步用户； |
| 用户 | 176 | 支持按照功能自定义用户角色，方便用户差异化使用需求； 支持对用户账号的自动化统计和异常展示，可展示的异常类型至少包含不活跃账号、已禁用账号、密码过期账号和账号过期账号； |
| 加密 | 177 | 对系统本身的数据加密方式支持国密四； |
| 管理视图 | ★ | 支持动态全景视图管理，管理员在设置好资产的层级关系后，系统可自动生成动态全景树状视图； |
| 资产管理 | ★ | 支持全面管理IPv6资产，即系统本身支持配置IPv6地址，也支持管理IPv6设备； |
| 工单申请 | 178 | 产品内置电子工单，满足运维人员或代维人员临时访问去求；支持密码工单管理，可通过工单申请相应资源的明文密码，审批通过后可通过邮件方式向申请人发送相应提示信息，有效期后平台会自动回收相应账号密码，并自动触发密码变更操作； |
| 密码管理 | 179 | 支持对Windows、linux、AIX、各种网络设备、数据库进行定期改密；改密后支持密码拨测功能，确认改密密码的正确性；支持等价资产管理和等价账号管理，当等价关系设定后，其中一台资产内的账号密码发生变更，等价的资产、账号密码随之自动变更； |
| 设备管理 | 180 | 支持对Windows设备访问的深度控制，包含但不限于控制磁盘映射、剪切板文本文件上传下载、远程桌面声音透传等；支持图形会话的自动TLS加密； |
| 命令行 | 181 | 支持对linux、AIX以及华为、思科、华三等字符设备的高危命令识别、限制功能，用户可自定义高危命令，高危命令匹配支持正则表达式；拥有先进性技术，能实现对各种非常规指令操作的100%识别； |
| 第三方导入 | 182 | 支持将运维用户提交的Excel设备访问文件导入系统中生成相应设备访问权限；支持灵活的设备访问授权方式，可以按照用户自定义的用户属性、设备属性等制作设备访问权限；协同运维：支持运维会话协同，可邀请其他用户参与、协助操作，会话协同过程中，支持参与者控制会话，同时支持创建者强制获取控制权，支持多个参与者使用相同的会话邀请链接进入会话； |
| 数据库 | 183 | 支持通过堡垒机，打开oracle客户端访问目标数据库时候的数据库连接限制，限制内容包含：OCI\_HOST、Service\_Name和OCI\_PORT；拥有先进性技术，实现有别于传统网络抓包方式的数据库审计（无需侦听网络流量），可支持的数据库类型包含：sqlserver、sybase和oracle； |
| 操作会话 | 184 | 支持同时输入多个关键字对用户操作会话进行精确定向审计；支持实时、自动展示在线会话数、在线用户数、会话大小统计等信息；支持图形操作的关键事件切片，管理员点击任意切片，即可直接定位到对应操作片段； |
| 传输功能 | 185 | 针对基于云盘模式的文件传输操作：用户将文件暂存在系统上，再经由系统，一键上传到目标系统或者一键下载到用户本地； 支持文件分享操作，且在系统web界面即可完成。无需通过第三方存储介质（如U盘）进行转储； |
| 负载功能 | 186 | 支持使用Windows2008、2012/2016作为应用发布服务器，同时支持配置多台应用发布服务器，多台应用发布服务器支持自负载均衡访问调用； |
| 扩展性 | 187 | 为满足未来性能要求，系统本身需要支持负载均衡，搭建集群时无需借助其它负载均衡设备；支持在系统的web页面部署HA和多A集群。 |

### 集中管理平台 1套

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 支持受控端管理数目 | ★ | 可管控≥2000个接入户数量 |
| 硬件规格 | ★ | 标准1U，≥6个千兆电口，≥1T SATA数据盘 |
| 软件功能 | ★ | 集中管理平台可以完成数据中心主要安全设备的集中管理，包括不限于防火墙，VPN，上网行为管理，安全感知等设备，包括多种Internet接入及专线接入的配置管理等，简化分支IT管理。 |
| 部署模式 | 188 | 设备必须支持单臂模式，以在不影响原有网络情况下同时能降低网络单点故障的发生概率。 |
| 底层虚拟化平台 | 189 | 支持并配置动态资源扩展功能，系统将自动评估虚拟机的性能情况，当虚拟机性能不足时自动为虚拟机添加CPU和内存资源 |
| 190 | 虚拟化内核基于KVM底层开发 |
| 191 | 支持配置内存回收机制，实现虚拟化平台内存资源的动态复用 |
| 192 | 支持无代理跨物理主机的虚拟机USB映射，需要使用USB KEY时，无需再虚拟机上安装客户端插件，且虚拟机迁移到其它物理主机后，仍能正常使用迁移前所在物理主机上的USB资源 |
| 193 | 支持分布式部署虚拟化平台 |
| 194 | 为获得良好的兼容性操作系统支持需要包括Windows、 Linux，并且支持国产操作系统包括不限于：红旗linux、中标麒麟、中标普华等 |
| 195 | 在可视化的WEB管理平台上，可以查看虚拟分布式存储对应的容量大小、容量使用率、实时的IOPS读写次数、IOPS读写数据量等信息，方便为IT管理做为有效的决策依据。 |
| 196 | 支持平台中的集群资源环境一键检测，包括系统运行状态检测（系统服务检测、配置文件检测、系统分区检测、存储空间检测）、系统配置检测（系列号有效性检测、网口配置检测）、硬件健康监测（CPU检测、内存检测、网卡检测、磁盘基本功能检测、RAID检测） |
| 197 | 支持数据数据重构功能，且重构速度可以达30min/TB |
| 198 | 支持在数据重构进行过程中，选择所需重构数据的优先级 |
| 199 | 可以支持手动指定路由器运行在固定的物理主机上，可以自动将路由器规划到高性能和高网络吞吐的物理主机上 |
| 软硬解耦 | 200 | 支持软硬件平台一体化交付，以及支持部署在其他虚拟化平台； |
| 可视化展示分支 | 201 | 具备可视化界面，以地图方式通过不同颜色展示全网分支机构健康、离线、告警状态，同时可展开省、市、区等多级分支。 |
| 设备自身管理 | 202 | 支持Web、SSH； |
| 远程接入分支 | 203 | 支持通过单点登录方式远程接入分支进行配置和管理。 |
| 网点区域管理 | 204 | 支持按用户组织结构及地域分布来新建受控网点区域，并实现网点区域的嵌套管理，更符合用户管理习惯。 |
| 网点快速部署 | 205 | 支持快速导入、导出网点信息，方便用户进行快速部署。 |
| 细致管理权限 | 206 | 支持按不同区域来指定不同的管理员，实现细化管理的同时防止管理员越权管理产生的混乱。 |
| 智能升级 | 207 | 智能监控分支端设备版本库，可设置升级计划，在某个时间段进行升级。 |
| 分支 | 208 | 支持展示所有在线网点的网络吞吐带宽展示、当前用户流量信息、分支设备版本信息；  支持即时查看受控设备状态，包括CPU、内存、磁盘占用等。  BBC智能监控分支端设备URL、应用识别库，若不是最新版本智能提醒升级。 |
| 告警 | 209 | 主机网口掉线、数据通信口不通、虚拟机与外部网络不通、直击网口丢包等。  分支设备离线  分支设备序列号过期、序列号状态异常、虚拟网络设备序列号过期等。  主机CPU、磁盘利用率高，虚拟网络设备CPU、磁盘利用率高等。  全网分支网络安全告警，如系统漏洞、攻击、木马等安全风险。 |
| BBC日志查看 | 210 | 内置日志中心，详细记录管理员操作日志，管理员也可自行设定过滤规则来查看所需日志信息。 |
| 上网行为日志 | 211 | 支持同步受控端数据中心的日志到同一个外置数据中心，支持对内网中所有受控端日志的统计、排行和导出； |
| 受控端设备日志查看 | 212 | 管理员通过BBC远程接入可以查看任何一台受控设备的实时及历史日志信息。 |
| 分支快速上线 | 213 | 支持通过BBC下发邮件方式，实现分支管理人员点击邮件链接即可实现分支自动互联BBC，简化分支配置，实现分支快速上线。 |
| 丰富的报表分析 | 214 | 支持展示分支资源利用率排行TOPN、分支带宽利用率TOP排行、分支告警问题总数趋势、分支告警排行TOP5、分支告警数量分布、分支离线市场TOP5等报表。 |

### 智能网管软件 1套

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| B/S架构 | ★ | 要求投标产品采用纯B/S架构，用户无需安装客户端，通过标准浏览器就能完成对系统的访问。 |
| 系统管理 | 215 | 支持通过WEB浏览器实现网管系统自身服务的重启、关闭；监控服务器自身的CPU、内存、网卡状态；支持在网页上获取系统运行日志 |
| 授权管理 | 216 | 支持文件授权方式 |
| 系统集成能力 | 217 | 支持将网管界面免登录方式被集成到客户的系统中;  支持将网管自身的告警、收到的SYSLOG、TRAP转发到客户的系统中;  支持透过WEBSERVICES接口，或者网管自身的资产、告警、性能数据; |
| 有线无线一体化管理 | ★ | 能够通过模块化、组件化方式，实现对网络中的路由器、交换机、WLAN等有线无线一体化管理。 |
| 组件扩展 | 218 | 支持无线网络业务 ，支持有线无线网络设备统一化管理和监测 |
| 设备管理 | ★ | 具备丰富的设备管理功能 ，包含对设备和设备接口及其信息的增删改查具有良好的展示和基本操作功能;  可以对多台设备进行批量的设备软件升级;  图形化显示设备的真实物理面板及线卡、端口信息，且支持在面板页面直接对设备进行操作;  能够自动对设备软件版本进行升级条件判断，支持设备软件版本的批量升级操作;  支持对设备的分权分级管理操作，可设置用户对单个或多个设备的只读、可写、不可见的权限，不可见设备须在拓扑图中有醒目标示;  支持对设备的机构名称、购买时间、质保期等资产信息进行编辑管理; |
| 设备配置管理 | ★ | 支持定时自动抓取设备的配置文件 ，同步到管理组件服务器，对每次采集内容都可与上一次采集到配置文件进行比对，出现偏差可邮件通知管理员。 |
| 219 | 具备以图形化向导的方式提供ACL ，QoS快速部署管理。 |
| 拓扑管理 | 220 | 自动发现网络中的二、三层网络设备，可以自动构成网络拓扑图  支持广域网链路的拓扑发现，且支持在拓扑图中添加“建筑物”、“云”等虚拟节点  可以通过指定IP段范围、设备选择等方式，显示“网络拓扑”的自定义拓扑视图，且在每一个视图中只能看到与该视图定义相匹配的设备。  支持路由拓扑自动发现，显示系统网络层设备之间的路由关系  支持当前拓扑图导出功能 |
| 221 | 可根据系统实时采集的设备和链路状态信息，动态更新网络拓扑图  支持双线STP链路检测，拓扑图可分别显示双线的实时状态  支持拓扑图的全屏显示模式 |
| ★ | 具备动画形式 主动推送拓扑告警信息的演示功能。 |
| 222 | 设备运行状态发生变化和触发告警时，拓扑图中的相应结点能够及时更改为醒目颜色  支持VSU拓扑，将设备的多虚一（VSU）状态实时呈现在拓扑图中，并可直接在拓扑图上呈现多个设备成员的链路连线和状态。  支持通过上传图片实现背景图自定义。  支持通过上传图片实现节点图标自定义。  支持WeatherMap模式的流量模式拓扑图。 |
| 实时告警功能 | 223 | 投标产品需要内置丰富的常见告警预定义类型，并可根据需要随时进行自定义所需告警类型的添加，提供至少10种以上常见SYSLOG告警类型预定义清单;  投标产品需要内置丰富的常见告警预定义类型，并可根据需要随时进行自定义所需告警类型的添加，提供Trap预定义告警类型大于等于50种以上预定义清单;  可以为监控的性能指标阈值设定为一般、重要和严重三级阈值 ，当性能指标超过阈值时，根据不同级别的阈值发送不同的告警提示;  支持针对流量的下限告警，当流量低于指定阈值时，也可以发告警出来;  支持设置指定设备的维护日程，在此维护日程时间段内，不会再发告警; |
| 关键链路检测功能 | 224 | 对关键链路的实时状态具备智能检测功能，若状态发生变化，能够智能快速的定位故障点，并支持以多种告警形式通知管理员。 |
| 报表管理 | 225 | 可定制监控任务，长期监控网络性能，支持即时生成报表、周期性生成报表;  具备报表的创建、查询、修改、删除功能，支持报表的在线浏览、报表导入导出等功能，支持周期性生成报表和定向发布功能;  支持历史报表的查询; |
| 接口映射关系管理 | 226 | 支持定期收集用户设备的IP、MAC、PORT映射表，当映射表发现异常时作为事件及时通知管理员。 |
| 拓扑融合用户信息 | 227 | 为了保障用户前期的投资，要求支持与SAM\SMP\ESS注册对接，实现查询在线用户列表，包括用户名、IP地址、MAC地址等功能 |
| 兼容性要求 | 228 | 要求投标产品支持标准的SNMP MIB信息管理库，支持主要厂商的标准MIB设备的监控管理。 |
| 配置要求 | ★ | 配置有线管理授权和无线管理授权；  支持有线网络管理节点≥3000，配置 1套有线网络管理节点授权：100个；  支持无线网络管理节点≥8000，配置 1套无线网络管理节点授权：200个。 |

### A类服务器 5台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 规格 | ★ | 机架式服务器，非OEM，带可调节机架安装导轨，高度≤2U；支持铂金、金牌、银牌等全系列 |
| CPU | ★ | CPU≥2颗Xeon Gold系列处理器或更好，CPU支持虚拟化技术；CPU核心数量≥16核心，CPU主频≥2.3GHz； |
| 内存 | ★ | 总容量≥512GB，单条内存容量≥32GB，内存单条为DDR4；  服务器支持20个DDR4 DIMM 插槽；  支持高级内存纠错（ECC）、内存镜像（Ememory mirroring）、内存热备（rank sparing）等功能 |
| 硬盘 | ★ | 支持SAS/SATA/NVMe接口，SSD数量≥10，SSD单硬盘≥1.92TB |
| RAID卡 | ★ | Cache≥2G，支持RAID0/1、RAID5、RAID10等功能，带电池或电容保护； |
| 网卡配置 | ★ | 10/100/1000自适应电口≥2，万兆多模光口网卡≥4（含4块万兆多模光模块），光模块支持数字诊断功能 |
| USB接口 | 229 | 服务器USB接口≥2 |
| 电源、风扇 | ★ | 热插拔冗余交流电源≥2、满配热插拔冗余风扇 |
| I/O扩展槽 | 230 | 支持≥6个PCI-E插槽 |
| 重要要求 | ★ | 配置设备远程管理功能，支持服务器监控和远程管理； |
| 一般要求 | 231 | 国标插头电源线，符合标准IDC机房要求；  支持兼容64位Windows Server、CentOS、Redhat； |

### B类服务器 14台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 规格 | ★ | 机架式服务器，非OEM，带可调节机架安装导轨，高度≤2U；支持铂金、金牌、银牌等全系列 |
| CPU | ★ | CPU≥2颗Xeon Gold系列处理器或更好，CPU支持虚拟化技术**；**CPU核心数量≥20核心，CPU主频≥2.5GHz； |
| 内存 | ★ | 总容量≥512GB，单条内存容量≥32GB，内存单条为DDR4；  服务器支持20个DDR4 DIMM 插槽；  支持高级内存纠错（ECC）、内存镜像（Ememory mirroring）、内存热备（rank sparing）等功能； |
| 硬盘 | ★ | 支持SAS/SATA/NVMe接口，SSD数量≥2，SSD单硬盘≥480GB |
| RAID卡 | ★ | Cache≥2G，支持RAID0/1、RAID5、RAID10等功能，带电池或电容保护； |
| 网卡配置 | ★ | 10/100/1000自适应电口≥2，万兆多模光口网卡≥6（含6块万兆多模光模块），光模块支持数字诊断功能 |
| USB接口 | 232 | 单服务器USB接口≥2 |
| 电源、风扇 | ★ | 热插拔冗余交流电源≥2、满配热插拔冗余风扇 |
| I/O扩展槽 | 233 | 支持≥6个PCI-E插槽 |
| 重要要求 | ★ | 配置设备远程管理功能，支持服务器监控和远程管理； |
| 一般要求 | 234 | 国标插头电源线，符合标准IDC机房要求；  支持兼容64位Windows Server、CentOS、Redhat； |

### C类服务器 6台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 规格 | ★ | 机架式服务器，非OEM，带可调节机架安装导轨，高度≤2U；支持铂金、金牌、银牌等全系列 |
| CPU | ★ | CPU≥2颗Xeon Silver系列处理器或更好，CPU必须支持虚拟化技术，CPU核心数量≥10核心，CPU主频≥2.2GHz； |
| 内存 | ★ | 总容量≥256GB，单条内存容量≥16GB，内存单条为DDR4  服务器支持20个DDR4 DIMM 插槽  支持高级内存纠错（ECC）、内存镜像（Ememory mirroring）、内存热备（rank sparing）等功能 |
| 硬盘 | ★ | 支持SAS/SATA/NVMe接口，系统盘配置SSD数量≥2，SSD单硬盘≥480GB，数据盘配置SSD数量≥12，SSD单硬盘≥1.92TB， |
| RAID卡 | ★ | Cache≥2G，支持RAID0/1、RAID5、RAID10等功能，带电池或电容保护； |
| 网卡配置 | ★ | 10/100/1000自适应电口≥2，万兆多模光口网卡≥4（含4块万兆多模光模块），光模块支持数字诊断功能 |
| USB接口 | 235 | 单服务器USB接口≥2 |
| 电源、风扇 | ★ | 热插拔冗余交流电源≥2、满配热插拔冗余风扇 |
| I/O扩展槽 | 236 | 支持≥6个PCI-E插槽 |
| 重要要求 | ★ | 配置设备远程管理功能，支持服务器监控和远程管理； |
| 一般要求 | 237 | 国标插头电源线，符合标准IDC机房要求；  支持兼容64位Windows Server、CentOS、Redhat； |

### D类服务器 9台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 服务器规格 | ★ | 机架式服务器，非OEM，带可调节机架安装导轨，高度≤2U；支持铂金、金牌、银牌等全系列 |
| CPU | ★ | CPU≥2颗Xeon Silver系列处理器或更好，CPU必须支持虚拟化技术，CPU核心数量≥10核心，CPU主频≥2.2GHz； |
| 内存 | ★ | 总容量≥256GB，单条内存容量≥16GB，内存单条为DDR4；  服务器支持20个DDR4 DIMM 插槽；  支持高级内存纠错（ECC）、内存镜像（Ememory mirroring）、内存热备（rank sparing）等功能 |
| 硬盘 | ★ | 支持SAS/SATA/NVMe接口，系统盘配置SSD数量≥2，SSD单硬盘≥480GB，缓存盘数量≥1,单硬盘≥3.2T NVME SSD缓存盘读写均衡型，数据盘数量≥12块单硬盘≥4TB SATA |
| RAID卡配置 | ★ | Cache≥2G，支持RAID0/1、RAID5、RAID10等功能，带电池或电容保护； |
| 网卡配置 | ★ | 10/100/1000自适应电口≥2，万兆多模光口网卡≥4（含4块万兆多模光模块），光模块支持数字诊断功能 |
| USB接口 | 238 | 单服务器USB接口≥2 |
| 电源、风扇 | ★ | 热插拔冗余交流电源≥2、满配热插拔冗余风扇 |
| I/O扩展槽 | 239 | 支持≥6个PCI-E插槽 |
| 重要要求 | ★ | 配置设备远程管理功能，支持服务器监控和远程管理； |
| 一般要求 | 240 | 国标插头电源线，符合标准IDC机房要求；  支持兼容64位Windows Server、CentOS、Redhat； |

### E类服务器 1台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 服务器规格 | ★ | GPU服务器产品为非OEM产品，≤4U机架式服务器，配置安装导轨。 |
| CPU | ★ | CPU≥2颗Xeon Gold系列处理器或更好，CPU必须支持虚拟化技术，CPU核心数量≥20核心，CPU主频≥2.1GHz； |
| 显卡（GPU） | ★ | 配置≥2块，单块显卡双精度≥7 TeraFLOPS，单精度≥14 TeraFLOPS，深度学习≥112 TeraFLOPS，双向互联带宽≥32 GB/s，显存≥32GB，显卡扩展槽≥8个 |
| 扩展插槽 | 241 | ≥6个标准PCI-E 3.0 插槽 |
| 内存 | ★ | 总容量≥512GB，单条内存容量≥32GB，内存单条为DDR4,最高支持 3TB DDR4 Ecc内存；服务器支持20个DDR4 DIMM 插槽 |
| 硬盘 | ★ | 支持SAS/SATA/NVMe接口,内置支持2个M.2 SATA SSD，其中最大可支持8个U.2接口NVME SSD；配置≥2块480GB SSD系统存储。配置≥4块1.92TB SSD存储。  配置≥2块480GB SSD系统存储。配置≥4块1.92TB SSD存储。配置SAS硬盘RAID后容量≥8TB。 |
| RAID卡配置 | ★ | Cache≥2G，支持RAID0/1、RAID5、RAID10等功能，带电池或电容保护； |
| 网卡配置 | ★ | 10/100/1000自适应电口≥4，万兆多模光口网卡≥2（含2块万兆多模光模块），光模块支持数字诊断功能 |
| USB接口 | 242 | 单服务器USB接口≥2 |
| 电源 | ★ | 配置2+2冗余电源模块，单块电源额定功率≤2200W |
| 风扇 | ★ | 配置冗余风扇 |
| 服务器监控管理功能 | 243 | 提供监控管理功能，包括服务器关键硬件组件监控、散热风扇速度、温度、指引灯诊断、电压等。 |
| 兼容性要求 | ★ | 兼容并行存储、集群管理软件、提供与兼容系统无偿技术支持，提供免费的系统集成支持。AI多机并行加速性能测试，测试至少两种深度学习框架，使用ImageNet图片集，测试模型采用AlexNet，或Resnet从1个GPU卡到16个GPU卡的性能，加速比≥14x |
| AI管理平台 | 244 | 支持商业版的集群管理或任务调度软件 |
| AI应用分析软件 | 245 | 支持商业版AI应用任务分析软件 |

### F类服务器 1台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 服务器规格 | ★ | GPU服务器产品为非OEM产品，≤4U机架式服务器，配置安装导轨。 |
| CPU | ★ | CPU≥2颗Xeon Gold系列处理器或更好，CPU必须支持虚拟化技术，CPU核心数量≥20核心，CPU主频≥2.1GHz； |
| 显卡（GPU） | ★ | 配置≥16块显卡，单块显卡单精度性能≥8.1 TFLOPS，混合精度≥65 TFLOPS，INT8 精度≥130 TOPS，INT4 精度≥260 TOPS，显存≥16GB |
| 扩展插槽 | 246 | ≥6个标准PCI-E 3.0 插槽 |
| 内存 | ★ | 总容量≥256GB，单条内存容量≥16GB，内存单条为DDR4,最高支持 3TB DDR4 Ecc内存；服务器支持20个DDR4 DIMM 插槽 |
| 硬盘 | ★ | 支持SAS/SATA/NVMe接口,内置支持2个M.2 SATA SSD，其中最大可支持8个U.2接口NVME SSD；  配置≥2块480GB SSD系统存储。配置≥4块1.92TB SSD存储。配置SAS硬盘RAID后容量≥8TB。 |
| RAID卡配置 | ★ | Cache≥2G，支持RAID0/1、RAID5、RAID10等功能，带电池或电容保护； |
| 网卡配置 | ★ | 10/100/1000自适应电口≥4，万兆多模光口网卡≥4（含4块万兆多模光模块），光模块支持数字诊断功能 |
| USB接口 | 247 | 单服务器USB接口≥2 |
| 电源 | ★ | 配置2+2冗余电源模块，单块电源额定功率≤2200W |
| 风扇 | ★ | 配置冗余风扇 |
| 服务器监控管理功能 | 248 | 提供监控管理功能，包括服务器关键硬件组件监控、散热风扇速度、温度、指引灯诊断、电压等。 |
| 兼容性要求 | ★ | 兼容并行存储、集群管理软件、提供与兼容系统无偿技术支持，提供免费的系统集成支持。AI多机并行加速性能测试，测试至少两种深度学习框架，使用ImageNet图片集，测试模型采用AlexNet，或Resnet从1个GPU卡到16个GPU卡的性能，加速比≥14x |
| AI管理平台 | 249 | 支持商业版的集群管理或任务调度软件 |
| AI应用分析软件 | 250 | 支持商业版AI应用任务分析软件 |

### 服务器机柜 3台

|  |  |  |
| --- | --- | --- |
| **指标项** | **重要性** | **指标要求** |
| 机柜规格 | ★ | 服务器机柜，≥600\*1200\*2000，≥19"/42U，黑色，前后网孔钢板门；内含接地端子，侧板可拆卸，内嵌式安全门锁，双路输入线缆连接采用工业连接器方式，单机柜配置≥2路PDU，单路PDU配置≥20个插孔,含≥2个16A插孔。 |

## 技术要求：

|  |  |  |
| --- | --- | --- |
| **序号** | **内容** | **需求说明** |
| 1 | 业务需求 | 本次项目建设是构建技术先进、安全稳定、功能区域划分清晰、模块化统一管理的互联网出口区域，建设完成后将为人民日报社提供统一的办公网、业务网信息化基础环境及互联网出口。 |
| 2 | 技术需求 | 互联网出口将配置包含访问控制、包过滤防护、上网行为控制、网络攻击防护及数据安全传输防护等安全措施，保障报社对外发布业务系统、办公网用户的网络安全访问。网络出口改造完成后能满足网络5-7年的技术发展需求。 |
| 3 | 系统需求 | （1）标准化。标准化是网络出口改造的基础保障，网络基础环境建设必须在网络结构、网络协议等标准方面遵循技术标准，同时在信息安全和通信路由方面充分考虑媒体行业规范。  （2）高可靠性。整个出口链路应有足够的冗余，设备发生故障时能以热备份，热切换和热插拔的方式在最短时间内加以修复。在方案设计过程中，必须对各个区域的部署进行合理的规划、保障系统全年不间断稳定运行，提高系统的可靠性。  （3）先进性。采用先进的体系结构、先进的系统软硬件平台，确保本系统起点高、技术领先。系统建设遵循结构化和模块化的设计，清晰的划分各个功能模块，且根据系统实际情况将各个模块集成为一个统一的网络平台，为各应用系统和办公上网提供良好的支持。 |

## 实施要求：

|  |  |  |
| --- | --- | --- |
| **序号** | **内容** | **实施标准** |
| 1 | 项目实施过程文档管理 | 投标人应针对本项目提供完整、详细的项目管理控制文档等。投标人应在项目完成时将本次项目的全部有关技术文件、图表资料及测试、验收报告等文档汇集成册及相应的电子版本交付招标人。投标人项目实施应依据等级保护相关要求和标准进行；投标人与招标人建立技术联络会制度，并根据用户要求定期组织召开项目沟通会，汇报项目进展情况。 |
| 2 | 项目实施进度安排 | 投标人应根据本文件中交付周期与时间要求，制定项目进度计划及资源保障计划，并按计划实施。 |
| 3 | 项目安装过程安排 | 投标人须提供详细的项目管理方案，包括项目管理方案及项目组织架构等内容，并在项目实施过程中，遵循甲方的相关技术要求，如需进入技术区工作时，应由招标人技术人员全程陪同，否则禁止任何操作。 |
| 4 | 项目验收安排 | 系统测试、验收包括初验、系统试运行和终验3个环节。项目完成现场软硬件安装调试工作后，用户方将组织初步验收，形成初验报告，经用户方、监理方、总集成方、投标人签字确认后，方可进入试运行阶段。试运行阶段期间，穿插进行用户培训，随后进入终验阶段。投标人需制定测试方案，并根据测试结果进行方案优化,同时针对试运行期间暴露的各类问题，按照用户方要求对系统进行必要的改进和完善，确保系统具备正式上线运行的条件。 |
| 5 | 项目培训安排 | 投标人在系统终验前根据用户方实际要求，制定详细培训计划，针对软、硬件系统，在固定场地对用户进行培训 |

## 服务要求：

### 服务总体要求

整个项目的实施工期分为需求调研及设计阶段、实施阶段、试用阶段、验收阶段、售后技术服务五个阶段，投标人投标时应对项目建设的每个阶段做出具体的分析与设计，投标人需充分了解人民日报社整体网络、安全平台架构，考虑技术方案与目前网络系统的融合性和未来整个系统的可扩充性，同时考虑到技术上的可靠性、先进性、适用性、完整性作为方案的设计原则，根据各采用设备的特点提出具体建议、实现方法和详细说明。项目实施进度应符合招标整体工期要求、对各阶段的时间安排计划、工作任务、工作重点、工作成果、验收标准等做出实质性响应。

投标人应成立相应的项目小组，并指定专职的项目经理，按照项目总集成团队及监理团队的要求，对项目进行组织协调和工程调度。

承诺函加盖投标人公章。投标人承诺在项目实施过程中全力支持项目总集成商、监理的工作，并配合协助项目的监理、总集成商完成整体项目的实施工作，包括并不限于设计方案、安装、测试、割接（网络安全系统割接，综合布线等实施方案）和调整更新、培训等。

承诺函加盖投标人公章。投标人承诺本次项目涉及的设备应有铭牌，线路应按规范布局并标注清晰准确，项目完工需提供详细连线图纸及相关技术说明文档。对设备的配置须具有详细的配置和维护文档手册，须具有详细的操作使用说明。

### 人员总体要求

承诺函加盖投标人公章。投标人需提供不少于3年的1人5\*8现场驻场服务，驻场人员负责本项目验收后的设备调试、策略调整及运维工作，驻场前需要经过招标人面试。

项目组团队制定项目实施计划，进行人员分工安排，按时、按质、按量完成招标人安排的工作，撰写系统配置文档。完成项目实施方案的编写工作及实施工作。

### 进度要求

1、设备及服务根据招标人要求采购并到货，其中设备需要在签订合同后10天内完成设备到货；

2、设备及服务在签订合同2个月内完成部署并开始试运行，试运行1个月经招标人确认合格后，正式验收。

3、投标人严格控制工作进度，按日制定详细的工作计划并在一天工作结束后向招标人提交当日工作进展情况报告。

## 安全保护措施要求：

投标人有义务在项目建设各阶段积极配合招标人发现和排除安全隐患，并由投标方拟定最终的安全保护措施文件，并经招标方确认。安全保护措施分为管理层面和技术层面二大部分：

（1）技术层面安全措施：

通过采取相关技术手段防止安全事故的发生，包括但不限于采取防木马病毒技术、防手机丢失或异常技术、防火墙技术、数据加密技术、登录验证技术、VPN技术、漏洞检测与在线黑客检测预警技术、数据存储技术、备份和安全恢复技术确保账号数据安全、系统安全、主机安全和传输安全；

（2）管理层面安全措施：

通过采取管理制度和其他物理措施防止安全事故的发生，如安全组织管理体系、高效能且职责分工明确的管理安全架构、业务组织体系和信息安全标准和评估体系。

## 设备到货验收要求：

### 总则

投标人在中标后应按供货合同中规定的到货时间和地点完成所有产品的到货及检验/检测工作。投标人应负责本标书要求的所有产品运输、交验、保险等一切费用。

对于投标人提供的产品，在供货时如有相应的版本升级产品，招标人保留更改产品版本的权力。

投标人提供的产品应支持与现有网络有良好的兼容性。

### 到货验收的基本要求

投标人必须保证是合同签订后最新出厂的产品；

依合同要求对产品的范围包括型号、规格、数量、货物包装、外观质量、软件介质、配件、货物装箱清单、原产地证明及货物质量检验合格证书等方面内容进行到货验收；确认无误后10个工作日内，甲乙双方签署《到货验收报告》。

当出现上述证明文件不完整或相关手续不全、到货验收时出现不是最新出厂的产品或不符合合同要求的严重质量问题时，招标人保留索赔及退货权利；

当出现产品及介质损坏、数量不全或产品不符等问题时，由投标人负责解决；产品检验/检测通过后，由招标人签署到货验收合格单。

### 到货验收程序

投标人应在合同规定的交货期内提供所有产品，在用户指定的安装地点进行产品交付。

1）所交付的产品应包括全部的介质、配件、相关资料以及装箱单等。

2）所交付的产品必须同时持有该产品合法的使用许可授权，其授权数应与用户要求相一致。

3）货物开箱后，目测产品应无损伤。

4）核对货物清单，检查交付货物的版本、数量以及相关配件。

5）货物外观受损，货物包括附件与合同货物清单或装箱单不符视为检验不合格。

6）投标人所提供的产品必须是全新的、无破损的，并为原厂包装，并符合规定的规格、质量、产地，如不符时，投标人应负责并免费更换全部不合格产品。

## 设备安装、调试、培训及验收要求：

### 安装调试要求

投标人在充分了解人民日报社的网络结构和网络使用需求的基础上，对设备的部署实施制定详细的实施方案，方案需经过招标人、监理、总集成商评审通过后方可进行实施。

投标人负责完成本项目所采购设备的到货、调试、验收、上架、安装、网络接入、操作系统安装配置；系统部署安装、测试上线所需的工具、网线/光纤、标签、扎带等耗材等由中标人负责提供，包含在投标报价中。

设备原厂商负责完成所供设备的配置和调试工作，包括安装配置、网络割接相关设置等工作。原厂商应派遣熟悉设备、经验丰富的技术专家和技术人员参加设备的现场安装施工，负责系统的调试、验收和割接开通，并对未能及时到场所引起的后果负责。

### 验收

项目验收分为三个阶段：

1．到货验收

所供设备全部到齐后，由招标人、监理、总集成商项目验收小组，对设备的品牌、配置、主要技术指标等进行核实、鉴定，逐项检查与投标文件中承诺的技术要求是否相符。签署《设备到货验收单》。

2．初步验收

设备安装调试完成后，从系统的可靠性、安全性、性能、稳定性、可管理性、可扩展性及规范实施、技术文档及注释说明等方面组织验收。验收应成立由招标人、总集成方，监理方、投标人以及其他有关人员组成的验收小组，负责对整个系统进行全面的验收。

投标人应针对本项目提供完整、详细的项目管理控制文档等。投标人应在项目验收时将本次项目的全部有关技术文件、图表资料及测试、验收报告等文档汇集成册及相应的电子版本交付招标人。

项目验收小组进行初步验收。验收合格后，系统开始试运行，签署《系统初验报告》。

3．最终验收

设备试运行1个月并具备竣工验收条件后，投标人须按照招标单位的要求，根据总集成单位及监理单位的验收标准组织测试验收，签署《系统最终验收报告单》。并向各方提供测试报告及项目验收材料、移交货物安装、运行、使用、测试、诊断和维修的技术文档，提供所购货物的安装指南、用户手册等项目成果。项目成果物应包含但不限于项目中产生的文档及相关质量证明文件。测试验收中如发现中标人虚假应答，招标人将上报有关主管单位，并要求中标人按合同约定赔偿招标人损失。

### 培训要求

合同签订后，对招标人技术人员进行专题基础技术培训；实施过程中对招标人技术人员进行现场操作培训；实施完成后对招标人技术人员进行专题使用维护培训。

投标人应提供培训方案，要列出培训课程、培训内容、达到的目标、培训对象和培训周期等。

投标人应制定一套科学、完整的系统日常监控、运维和操作文档；向招标人提供全套规范的技术文件，并与实际系统环境一致，包含安装手册、用户手册、系统管理手册、实施安装调试技术文档等。

投标人及原厂商培训教员的食宿及往返费用由投标人承担

## 售后服务要求：

自项目终验合格之日起，投标人须提供5年原厂免费维保服务（提供原厂售后服务承诺函），质保期内投标人要保修除消耗品以外的所有设备。五年质保期内包括不限于技术支持服务，硬件整机质保及软件升级服务。投标人必须为投标文件中所提供和安装的软、硬件产品提供7\*24小时专人负责的服务。具体详细要求如下：

### 技术支持服务

服务期内，接到招标人请求后，设备原厂商应提供以下形式的技术支持服务：

（1）电话咨询

设备原厂商提供本次采购设备（含系统软件）的质量保障服务，为用户提供7\*24小时技术支持电话，解答用户在系统使用中遇到的问题，及时提出解决问题的建议和操作方法电话咨询。

（2）远程在线诊断和故障排除

对于电话咨询解决不了的问题，经招标人授权设备原厂商可通过互联网远程登录到用户网络系统进行故障诊断和故障排除。

（3）现场响应

提供7\*24原厂商软硬件质量保障服务，收到招标人的服务请求后，服务响应时间不得超过0.5小时，设备原厂商应指派技术人员在2小时内赶赴现场进行故障处理，。

（4）保障服务

投标人及原厂商提供特殊时段（如两会期间、国庆节、不定期重大会议安保期间、系统停机维护及用户认为必须的重要时段）的提供驻场技术支持服务，不另行收费。

### 硬件整机质保

备件备品：投标人承诺所投产品在北京已建立足够的售后服务机制，配备有足够的备品备件，能够按质保服务要求为招标人及时提供原厂技术支持和备件更换服务。投标人及原厂商保证所提供设备的备件库可以满足招标人日常使用、排除硬件故障、升级的需求。质保期内，投标人及原厂商免费以全新配件更换正常使用下损坏的配件，并提供免备件费、免人工费、免服务费的故障备件更换服务。

软件服务：提供所购设备自带及选配软件的使用支持服务，且不影响免费质保期。 在质保期内对所有涉及软件使用方面的技术支持不另行收费。

兼容解决：若投标人及原厂商所提供设备同与之相关联的硬件、软件产品出现兼容性问题时，投标人及原厂商须积极配合，与有关硬件、软件厂商和招标人接洽，及时定位问题原因、寻求解决方案。

设备移机：在免费质保期内设备移机（物理迁移），投标人及原厂商根据招标人需要，提供现场支持服务。服务不另行收费，不影响质保期。

升级支持：投标人及原厂商免费为招标人提供本次采购的系统软件维护、版本升级、微码升级、补丁程序及技术支持等服务，保证设备软硬件系统正常运行。

### 软件升级服务

在质保期内，投标人及原厂商免费为招标人提供本次采购的系统软件维护、版本升级、微码升级、补丁程序及技术支持等服务，保证设备软硬件系统正常运行，提供免费升级及更新服务。

## 保密要求：

投标人在中标后需签订保密协议，因项目获知招标人的网络结构、信息系统配置、系统账号及口令、IP地址等信息均应严格保密，不得在任何时间以任何理由向第三方泄露或用作其他用途。如违反保密要求造成泄密的，招标人将追究投标人相应的法律责任。