**对外政务信息服务平台硬件采购（交付/到货日期：合同签订后2周）**

## 一、设备列表（具体参数需求参见附表，须提供技术偏离表）

1、

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 数量 | 单位 | 分包 |
| 1 | 服务器一 | 26 | 台 | 包一 |
| 2 | 服务器二 | 10 | 台 |
| 3 | 服务器三 | 75 | 台 |
| 4 | 融合一体机 | 1 | 套 |
| 5 | 存储一 | 3 | 套 |
| 6 | 存储二 | 2 | 套 |
| 7 | 存储三 | 3 | 套 |
| 8 | SDN控制器 | 1 | 套 |
| 9 | 数据中心交换机一 | 2 | 台 |
| 10 | 数据中心交换机二 | 3 | 台 |
| 11 | 汇聚交换机 | 2 | 台 |
| 12 | 接入层交换机 | 30 | 台 |
| 13 | 存储光纤交换机一 | 6 | 台 |
| 14 | 存储光纤交换机二 | 1 | 台 |
| 15 | POE交换机 | 10 | 台 |
| 16 | 万兆防火墙 | 2 | 台 |
| 17 | 安全网关 | 2 | 台 |
| 18 | 堡垒机 | 1 | 台 |
| 19 | 网络准入网关 | 1 | 台 |
| 20 | 应用负载均衡 | 2 | 台 |
| 21 | 数据库审计 | 1 | 台 |
| 22 | 入侵监控软件 | 30 | 套 |
| 23 | 内网文件管控系统 | 1 | 套 |
| 24 | 协议分析仪 | 1 | 套 |
| 25 | 邮件防火墙 | 1 | 台 |
| 26 | 杀毒软件 | 1 | 套 |
| 27 | 域名解析设备 | 1 | 台 |
| 28 | 高密度无线AP | 3 | 台 |
| 29 | 蓝牙无线AP | 10 | 台 |
| 30 | 无线面板AP | 26 | 台 |
| 31 | 300M无线AP | 31 | 台 |
| 32 | VPN设备 | 2 | 台 |
| 33 | 盘柜 | 1 | 套 |
| 34 | 邮件归档系统 | 1 | 套 |
|  | | | | |
| 35 | 监控显示屏4K | 20 | 台 | 包二 |
| 36 | 监控工作站 | 4 | 台 |
| 37 | 移动工作站 | 5 | 台 |

## 二、参数要求（以下为各项的详细参数要求，＃项为关键指标）

### 服务器（单台）

|  |  |  |
| --- | --- | --- |
| **指标项** | | **指标要求** |
| 通用配置 | 规格 | 机架式服务器≤2U，带导轨 |
| **＃**处理器 | 处理器≥2颗，主频≥2.1GHz，核心≥8；三级缓存≥20MB |
| 内存插槽 | ≥24个内存插槽支持DDR4 ECC RDIMM/LRDIMM，支持内存镜像、内存热备 |
| 硬盘扩展 | 出厂扩展盘位≥28块2.5寸SAS/SATA/SSD热插拔硬盘，支持≥2块PCI-E SSD硬盘，支持SAS/SATA硬盘、SSD混插 |
| **＃**网络 | ≥2个千兆以太网网口，可支持万兆网卡，支持IOAT2高级网络加速功能和VMDq虚拟化加速功能，支持网络唤醒、网络冗余、负载均衡等高级网络特性 |
| Raid卡 | 配置2GB Cache、12Gb RAID控制器，支持RAID0/1/5/10/50，支持电容掉电保护 |
| I/O插槽 | ≥8个PCI-e 3.0插槽 |
| 显卡 | 集成带16MB显存的显示控制器 |
| 电源 | 1+1冗余白金电源 |
| 服务器一 | **＃**内存 | 内存≥256G DDR4 ≥2400MHz，ECC RDIMM |
| **＃**硬盘 | 硬盘≥4块 600GB 10000rpm 2.5寸 SAS热插拔 |
| 服务器二 | **＃**内存 | ≥128GB DDR4 ≥2400MHz，ECC RDIMM内存 |
| **＃**硬盘 | ≥4块 240G 2.5寸 6Gb/s SSD硬盘 |
| 服务器三 | **＃**内存 | ≥32G DDR4 ≥2400MHz，ECC RDIMM内存 |
| **＃**硬盘 | ≥4块300G 2.5寸10K SAS硬盘 |

### 融合一体机（单套）

| **指标项** | | **指标要求** |
| --- | --- | --- |
| 云平台层 | 基本要求 | 国产非oem品牌，所投虚拟化软件提供资源，服务，资产，监控，告警，记账，用户，管理等功能。 |
| 所投虚拟化软件支持GB18030-2005编码标准。 |
| 提供基于物理CPU的License以及相应的管理软件，许可与CPU的内核数量无关。 |
| 采用裸金属架构，无需绑定操作系统即可搭建虚拟化平台。Hypervisor结构精简，部署后所占用的存储空间在200M以下。 |
| 兼容性要求 | 软硬件为同一厂商品牌,支持主流x86服务器 |
| 虚拟化平台在部署Hypervisor后无需额外安装管理中心组件情况下，即可实现基于Web页面的平台访问和精细化管理功能。 |
| 功能性要求 | 提供虚拟机HA功能。 |
| 支持跨数据中心在线复制，迁移，可实现远距离无中断实时迁移工作负载。 |
| 支持将运行在平台上的应用程序打包成应用容器，并提供开启，关闭，克隆，共享等功能，为用户设计业务蓝图（BluePrint）。 |
| 支持16 Gb端到端光纤通道。 |
| 提供物理主机级别的无状态防火墙，无需使用IPTABLES，管理员可以用命令行和图形化界面配置防火墙。 |
| 提供存储由精简置备转为厚置备，从而提高存储性能，提高利用率。 |
| 虚拟机可以被外部存储阵列识别，实现基于存储策略的管理(SPBM)，可允许跨存储层实现管理以及动态存储类服务自动化，可实现按虚拟机级别的数据服务(快照、克隆、远程复制、重复数据消除等) 。 |
| 提供业务不中断的虚拟机存储的动态扩展功能。 |
| 扩展性 | 每个控制台可管理至少1000台物理服务器、10000台已打开电源的虚拟机，15000台已注册的虚拟机，并可以通过链接至少10个控制台实例，跨10个实例管理30000个已打开电源的虚拟机和50000个已注册的虚拟机。 |
| 无需单独部署计算、存储、网络管理组件，即可通过一套系统进行统一管理。 |
| 支持对包括虚拟机模板、ISO映像和脚本在内的内容进行存储库统一存储。用户可以从集中化位置存储和管理内容,以及通过发 / 订阅模型共享内容。  提供VMware环境到CloudVirtual环境的无缝实时迁移，保证业务连续性。  可以支持Web Client和命令行管理功能。 |
| 分布式存储层 | 基础要求 | 嵌入虚拟服务器内核，缩短I/O数据路径降低延时，虚拟服务器的CPU资源占用小于10%，与虚机的迁移无缝集成； |
| 由管理虚拟服务器的虚拟化管理中心统一配置、管理，支持Web界面 |
| 提供基于存储策略的管理机制，根据业务应用的需求，可以通过变更存储策略进行在线的动态调整业务应用正在使用的存储资源； |
| 可实现以虚拟机为中心的快照和克隆,支持每个虚拟机不少于32个快照和克隆； |
| 分布式存储管理软件支持的混合存储架构中，最大IO性能不少于4万IOPS/主机，200万IOPS/集群；  提供基于物理CPU的License以及相应的软件许可，许可与CPU的内核数量无关。 |
| 高可用性 | 无缝集成虚拟化平台的HA、多核虚拟机FT容错、虚拟机在线迁移、存储在线迁移、自动化资源调度等功能，无需额外安装软件； |
| 可利用分布式RAID和缓存镜像来确保在发生磁盘、主机、网络或机架故障时绝不丢失数据； |
| 无缝集成虚拟化备份以及容灾技术，RPO不大于5分钟。 |
| 兼容性要求 | 支持写密集型和读密集型SSD，支持ULLtra DIMM SSD和NVMe SSD，实现小于5微妙的写入延迟；  具有广泛的兼容性，支持现有市场上的主流x86服务器、I/O控制器、磁盘等，具有双方认可的官方硬件兼容性列表，包括但不限于IBM、HP、DELL、Cisco、NEC、Intel、SuperMicro、Fusion-IO、富士通、浪潮、华为、联想、曙光等 |
| 扩展性 | 分布式存储管理软件支持存储容量上限不少于8PB；  分布式存储管理软件最大可支持SSD磁盘数不少于320块，读写缓存支持动态扩展。 |
| 一体机机箱 | 基本要求 | 19寸标准机架式刀片机箱；支持8片以上双路计算节点或者4片以上存储节点；支持计算节点和存储节点混插；支持前维护。  实配4片双路计算节点和2片存储节点 |
| 参数配置 | 配置4个1200W白金牌效率的热插拔电源模块，可实现电源模块的2+2或3+1冗余；支持240V HVDC和220V AC，支持冷备份工作模式；支持400W BBU电池单元，提供二次备援功能； |
| 配置5组冗余热插拔风扇模块，实现4+1冗余； |
| 存储节点 | 基本要求 | 半高双路节点，同一个刀片机箱可支持≥4个； |
| **＃**参数配置 | ≥2颗Intel Xeon E5-2630v4系列，每颗CPU核心数≥10核，每颗CPU主频≥2.2GHz； |
| 配置≥128GB DDR4 2133MHz ECC RDIMM内存，≥16个内存插槽，最大可支持512GB内存，支持内存保护、内存镜像、内存热备； |
| 单存储节点支持≥2块2.5寸SAS、SATA、SSD热拔插硬盘和≥12块3.5寸SATA/SAS热插拔硬盘； |
| 配置≥2块800G 2.5寸6Gb/s SSD硬盘，≥10块2.5寸 900G 10K SAS硬盘，≥1块150G SATA SSD硬盘 |
| 其它参数 | 配置SAS 12Gb硬盘控制器，支持RAID 0/1/10 |
| 配置≥2个GE网口（电口），≥2个10GE网口（光口） |
| 不少于后置2个半高pcie3.0x8扩展插槽； |
| 板载BMC管理芯片，符合IPMI2.0标准的管理功能，并提供远程iKVM，Virtual Media功能 |

### 存储一（单套）

|  |  |  |
| --- | --- | --- |
| 指标项 | | 指标要求 |
| 控制器 | 架构 | 实际配置存储控制器≥2个（不包括外接虚拟化网关或NAS控制器等）；支持故障下自动切换，此时系统性能不下降、业务不中断、数据不丢失 |
| 集群能力 | 支持存储集群功能，可扩展控制器≥16个，双控制器硬盘数量≥3600块，提供证明材料 |
| 主机接口 | 实际配置16Gbps光纤接口≥8个、10Gbps以太网接口≥4个 |
| 授权许可 | 对以下提及的全部软件功能，实际配置最大容量授权及足额多路径软件许可证；未来扩容或增加主机连接时，无需追加此类授权及许可费用。 |
| 协议 | 配置SAN和NAS多种数据方式访问 |
| 缓存 | DDR4缓存 | 实际配置DDR4缓存≥512GB |
| SSD缓存 | 实际配置SSD缓存≥5.76TB |
| 缓存保护 | 配置数据断电保护 |
| 磁盘 | 可用容量 | 900GB或以上10000转SAS硬盘≥48块；6TB或以上7200转SAS硬盘≥26块 |
| 热插拔支持 | 支持磁盘热拔插和在线故障更换 |
| RAID保护 | 支持RAID 0、1、10、5、6等；优选可防范同RAID组内2块或以上磁盘故障的RAID类型；故障发生时，业务不中断、数据不丢失 |
| 故障重建 | 实际配置RAID快速重建功能，且重建过程中，性能不下降 |
| 软件功能 | 精简配置 | 实际配置精简配置功能；可根据数据卷组灵活进行全配置调整；使用精简配置功能不影响存储系统性能。 |
| 数据压缩 | 支持在线数据压缩功能 |
| 数据快照 | 实际配置基于时间点的数据快照功能 |
| 数据容灾 | 实际配置基于IP的数据复制功能； |
| 数据克隆 | 支持基于时间点快照的可写数据克隆功能 |
| QoS服务 | 支持基于数据卷组的QoS管理功能 |
| 兼容性 | 主机操作系统 | 支持Windows、Solaris、HP-UX、IBM-AIX、Linux、ESX等主流操作系统，支持OpenStack Cinder，提供原生容器支持。 |
| 系统管理 | 异构虚拟化 | 采用开放方式，支持异构存储虚拟化功能，能够实现多品牌存储在硬件或软件虚拟化网关下统一管理。 |
| 存储管理软件 | 采用开放存储管理软件，开放MIB及API接口，支持功能特性植入和二次开发； |
| 告警管理 | 配置日志告警、指示灯告警、控制台告警、蜂鸣器告警、邮件告警支持功能，支持故障事件和告警联动方式自定义 |
| 全面支持IPv6 | 配置IPv4/v6协议授权，可以通过IPv4/v6协议进行存储访问、带外管理、远程复制等。 |
| 多设备全局运维软件 | 配置图形化管理平台软件；配置多台存储系统统一监控管理功能、性能监控及趋势分析功能、容量监控及趋势分析功能、数据传输监控及压力分析功能；配置图形化呈现及分析能力。  能够同时管理多台存储设备。 |

### 存储二（单套）

|  |  |  |
| --- | --- | --- |
| 指标项 | | 指标要求 |
| 控制器 | 架构 | 实际配置存储控制器≥2个（不包括外接虚拟化网关或NAS控制器等）；支持故障下自动切换，此时系统性能不下降、业务不中断、数据不丢失 |
| 扩展能力 | 支持存储集群功能，可扩展控制器≥16个，双控制器硬盘数量≥960块，提供证明材料 |
| 主机接口 | 实际配置16Gbps光纤接口≥8个、10Gbps以太网接口≥4个 |
| **＃**性能要求 | 满足SPC-1 Revision 3.0以上版本IOPS≥40万，提供证明材料 |
| 授权许可 | 对以下提及的全部软件功能，实际配置最大容量授权及足额多路径软件许可证；未来扩容或增加主机连接时，无需追加此类授权及许可费用。 |
| 协议 | 配置SAN和NAS多种数据方式访问 |
| 缓存 | DDR4缓存 | 实际配置DDR4缓存≥256GB |
| SSD缓存 | 实际配置SSD缓存≥2.88TB |
| 缓存保护 | 配置数据断电保护 |
| 磁盘 | 可用容量 | 900GB或以上10000转SAS硬盘≥42块；4TB或以上7200转SAS硬盘≥16块 |
| 热插拔支持 | 支持磁盘热拔插和在线故障更换 |
| RAID保护 | 支持RAID 0、1、10、5、6等；优选可防范同RAID组内2块或以上磁盘故障的RAID类型；故障发生时，业务不中断、数据不丢失 |
| 故障重建 | 实际配置RAID快速重建功能，且重建过程中，性能不下降 |
| 软件功能 | 精简配置 | 实际配置精简配置功能；可根据数据卷组灵活进行全配置调整；使用精简配置功能不影响存储系统性能。 |
| 数据压缩 | 支持在线数据压缩功能 |
| 数据快照 | 实际配置基于时间点的数据快照功能 |
| 数据容灾 | 实际配置基于IP的数据复制功能 |
| 数据克隆 | 支持基于时间点快照的可写数据克隆功能 |
| QoS服务 | 支持基于数据卷组的QoS管理功能 |
| 兼容性 | 主机操作系统 | 支持Windows、Solaris、HP-UX、IBM-AIX、Linux、ESX等主流操作系统，支持OpenStack Cinder，提供原生容器支持。 |
| 系统管理 | 异构虚拟化 | 采用开放方式，支持异构存储虚拟化功能，能够实现多品牌存储在硬件或软件虚拟化网关下统一管理。 |
| 存储管理软件 | 采用开放存储管理软件，开放MIB及API接口，支持功能特性植入和二次开发； |
| 告警管理 | 配置日志告警、指示灯告警、控制台告警、蜂鸣器告警、邮件告警支持功能，支持故障事件和告警联动方式自定义 |
| 全面支持IPv6 | 配置IPv4/v6协议授权，可以通过IPv4/v6协议进行存储访问、带外管理、远程复制等。 |
| 多设备全局运维软件 | 配置图形化管理平台软件；配置多台存储系统统一监控管理功能、性能监控及趋势分析功能、容量监控及趋势分析功能、数据传输监控及压力分析功能；配置图形化呈现及分析能力。  能够同时管理多台存储设备。 |

### 存储三（单套）

|  |  |  |
| --- | --- | --- |
| 指标项 | | 指标要求 |
| 物理及电气规格 | | 机架式，冗余电源及风扇 |
| 控制器 | 架构 | 实际配置存储控制器≥2个（不包括外接虚拟化网关或NAS控制器等）；支持故障下自动切换，此时系统性能不下降、业务不中断、数据不丢失。 |
| 扩展能力 | 支持存储集群功能，可扩展控制器≥8个，控制器成对扩展后，性能线性增加。 |
| 主机接口 | 实际配置16Gbps光纤接口≥4个、10Gbps以太网接口≥4个 |
| 授权许可 | 对以下提及的全部软件功能，实际配置最大容量授权及足额多路径软件许可证；未来扩容或增加主机连接时，无需追加此类授权及许可费用。 |
| 协议 | 配置SAN和NAS多种数据方式访问 |
| 缓存 | DDR4缓存 | 实际配置DDR4缓存≥80GB |
| SSD缓存 | 实际配置SSD缓存≥1.44TB |
| 缓存保护 | 配置数据断电保护 |
| 磁盘 | 可用容量 | 900GB或以上10000转SAS硬盘≥14块；4TB或以上7200转SAS硬盘≥13块 |
| 热插拔支持 | 支持磁盘热拔插和在线故障更换 |
| RAID保护 | 支持RAID 0、1、10、5、6等；优选可防范同RAID组内2块或以上磁盘故障的RAID类型；故障发生时，业务不中断、数据不丢失 |
| 故障重建 | 实际配置RAID快速重建功能 |
| 软件功能 | 精简配置 | 实际配置精简配置功能；可根据数据卷组灵活进行全配置调整；使用精简配置功能不影响存储系统性能。 |
| 数据压缩 | 支持在线数据压缩功能 |
| 数据快照 | 实际配置基于时间点的数据快照功能 |
| 数据容灾 | 实际配置基于IP的数据复制功能 |
| 数据克隆 | 支持基于时间点快照的可写数据克隆功能 |
| QoS服务 | 支持基于数据卷组的QoS管理功能 |
| 兼容性 | 主机操作系统 | 支持Windows、Solaris、HP-UX、IBM-AIX、Linux、ESX等主流操作系统，支持OpenStack Cinder |
| 系统管理 | 异构虚拟化 | 采用开放方式，支持异构存储虚拟化功能，能够实现多品牌存储在硬件或软件虚拟化网关下统一管理。 |
| 存储管理软件 | 采用开放存储管理软件，开放API接口，支持功能特性植入和二次开发； |
| 告警管理 | 配置日志告警、指示灯告警、控制台告警、邮件告警支持功能，支持故障事件和告警联动方式自定义 |
| 全面支持IPv6 | 配置IPv4/v6协议授权，可以通过IPv4/v6协议进行存储访问、带外管理、远程复制等。 |
| 多设备全局运维软件 | 配置图形化管理平台软件；配置多台存储系统统一监控管理功能、性能监控及趋势分析功能、容量监控及趋势分析功能、数据传输监控及压力分析功能；配置图形化呈现及分析能力。  能够同时管理多台存储设备。 |

### SDN控制器

| 功能模块 | 指标项 | 指标要求 |
| --- | --- | --- |
| 统一管理平台 | 系统兼容性 | 可以支持Windows、Linux平台及MS SQL、Oracle等数据库，支持B/S架构。 |
| 部署方式 | 可以支持多服务器分布式虚拟化部署，可实现负载分担；支持双机热备、冷备等模式。 |
| 开放性 | 支持Restful API标准北向接口，可与第三方系统灵活对接。 |
| 向导式配置模式 | 提供向导式配置界面 |
| 自动化部署 | 将设备按核心、分支、接入进行分组，每个分组对应一份配置，通过配合DHCP实现配置完全下发。 |
| 可视化自动上线 | 支持通过图形界面方式规划网络拓扑，并展示设备自动上线过程。 |
| 全网资源管理 | 支持路由器、交换机、无线、安全、语音、存储、监控、服务器、打印机、UPS等设备进行管理，实现设备资源的集中化管理。管理员可以通过该功能根据业务需求创建设备组视图，并将所需设备加入该视图中进行管理。 |
| 拓扑管理 | 提供多种拓扑视图。 |
| IP管理 | 提供IP地址统计、查找功能。  管理员能够通过IP地址分配情况统计图表和查询整个网络的IP地址资源使用情况。 |
| 基于用户网络资源编排 | 支持基于用户以及用户组进行网络资源编排，实现用户以及用户组和网络属性VLAN、VXLAN、IP网段、IP地址的绑定。 |
| 图形化策略定义 | 提供集中化的界面配置组间策略矩阵，支持拖拽方式实现策略部署，并自动统一下发到所有的策略执行点。用户移动时无需修改配置，策略保持不变，实现策略随行。 |
| 隔离域编排 | 通过统一的用户编排实现用户及用户组接入时自动识别用户所属组，并将接入终端自动划入到相应的VRF隔离域。 |
| 物联终端的接入 | 通过统一的用户编排界面实现物联网终端接入时自动识别终端，并将接入终端按照业务应用自动划入到相应的VRF隔离域。 |
| 用户IP绑定 | 可以实现对DHCP服务器进行编排控制，配合基础网络实现用户组绑定IP网段、用户名绑定IP地址。 |
| Overlay网络管理 | 提供VXLAN业务管理，可以自动识别并导入VTEP设备，自动识别网络中的VXLAN和隧道，并实现对VXLAN的加入监控、移除监控、查看分层拓扑、查看业务拓扑、查看全网拓扑、查看详细信息和查看流量信息等功能。 |
| 性能 | 提供基于任务的性能监控，可定制监控任务，形成日/周/月报等报表。支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警。 |
| 合规 | 提供合规检查，可以简单方便的检查网络是否满足定制的法规，并提供修复功能，可以及时解决在网络环境中出现的配置、安全问题。 |
| 管理授权数量 | ≥50个节点 |
| 接入认证管理 | 接入用户管理 | 支持对用户的AAA认证管理。 |
| 多种802.1X接入认证 | 支持PAP认证、CHAP认证、EAP-MD5认证、EAP-PAP认证、EAP-TLS认证、EAP-PEAP-MSCHAPV2认证、EAP-PEAP-MD5、EAP-GTC、EAP-TTLS认证，防客户端破解。 |
| 哑终端接入自动化上线 | 根据事先导入系统的各类哑终端MAC地址列表，实现哑终端的自动化上线，自动完成对接入层设备、汇聚层设备的配置下发，实现专网隔离、即插即用效果。 |
| 智能终端认证页面定制 | 定制页面包括认证（或者注册）页面和处理结果页面，根据显示屏幕分为PC、PAD和手机多种页面类型。预置多套模板方便管理员通过可视化手段绘制页面，也可导入第三方定制的页面。 |
| RADIUS认证 | 支持RADIUS漫游认证，可对漫游用户在线查看和接入明细日志查询；无需终端用户输入用户名和密码；支持证书、多级证书认证和无线的WAPI认证方式。 |
| LDAP认证 | 支持从LDAP服务器上同步账户信息，支持的LDAP服务器包括：Microsoft Active Directory、Novell Directory Server、Netscape iPlanet、SUN ONE Directory、OpenLDAP等；支持LDAP服务器主备模式；支持实时与本地LDAP认证；支持自动、手工和按需同步账户信息；支持AD域控组用户，支持AD域控密码控制。 |
| 动态VLAN下发 | 可以在认证通过后下发用户VLAN，用户会自动进入其安全组对应的逻辑网络。 |
| 访客无感知认证 | 提供访客一次接入，多次使用的无感知认证。 |
| 用户自助管理 | 可通过自助平台进行预注册申请，管理员审核后即可开通用户帐号，用户可以通过自助平台对自己的用户信息进行管理，如查询、修改、密码设置、密码重新获取等；用户自助页面支持自定义。 |
| 访客行为审计 | 提供“黑名单”管理，可以将恶意猜测密码的访客加入黑名单，并可按MAC、IP地址跟踪非法行为的来源。支持管理员可以实时监控在线访客，强制非法访客下线。提供用户接入明细日志。 |
| 支持不同的访客账号创建方式 | 支持公共领域访客短信认证模式、访客接待员手工开户模式、访客自助开户模式。 |
| 用户组管理 | 关联接入策略和接入场景，用户组中的用户在不同的场景下应用不同的接入策略。 |
| 多种终端识别技术 | 支持通过客户端、DHCP、HTTP、MAC地址等技术准确识别接入网络的终端厂商、终端类型和操作系统信息。 |
| 基于场景的终端网络接入授权 | 支持根据终端接入区域、接入时间段、终端IP地址、终端MAC地址、终端厂商、终端操作系统和终端类型等对网络接入终端授予不同的访问权限。 |
| **＃**认证授权数量 | ≥3000节点 |
| 无线管理 | 支持无线定位 | 支持对移动用户、Rogue移动用户及Rogue AP进行定位；根据设定的规则，在位置拓扑上划分区域，并指定区域内允许或禁止接入的用户列表，如果进入禁止区域，可触发告警或阻断用户接入 |
| 无线用户信息管理 | 通过第三方Radius系统配合，能够关联移动用户MAC地址和账号的对应关系，并能够维护移动用户的账号信息。 |
| 系统支持无线资源与用户的统一管理 | 可在拓扑上对终端进行强制用户下线、下发消息、安全检查、加入黑名单、查看用户详细信息等功能 |
| 支持对移动终端设备类型进行识别 | 根据时间，地点，终端类型，SSID，身份、状态给不同终端不同网络访问权限 |
| 支持蓝牙、微波炉等干扰源的实时检测 | 支持丰富的频谱分析图表，包括实时FFT图，duty cycle图，信道利用率图以及信道质量图等,支持历史频谱数据的保存和回放,支持干扰源位置定位 |
| 支持AP接入端口管理 | 支持PoE功能的设备，可通过对PoE供电功能的操作控制AP的重启 |
| 支持GIS视图 | 用户可以自定义热点在地图上的显示位置 |
| 能查看各移动终端的全部漫游记录 | 位置视图可形象的通过动画查看用户漫游轨迹。 |
| 绿色节能管理 | 可按指定时间控制无线射频的开闭；可按指定时间控制AP、SSID、PoE的开闭 |
| 无线网络质量评估 | 通过人性化的优化向导设置，建立网络评估任务对无线网络运行状况进行评估，了解WLAN网络运行状况；生成基于拓扑，AP，终端三个维度的网络优化报告，发现薄弱区域，确认需要补点的位置 |
| 支持丰富的报表 | 包括移动用户Session统计报表、移动用户在线统计报表、移动用户在线趋势报表、AP在线用户数TopN报表、AP关联统计报表、Fat AP流量明细报表、Fat AP流量汇总报表、AP可用率明细报表、AP可用率汇总报表、AP退服明细报表、AP退服汇总报表、Radio速率统计报表，Radio流量统计报表、Radio错误统计报表、Radio资源利用率统计报表、Rogue AP统计报表、Rogue移动用户统计报表 |
| 支持查看AC与AP之间真实物理链路连接 | 真实显示从AP到PoE交换机、三层交换机、路由器等物理链路 |
| **＃**管理AP授权数量 | ≥50节点 |

数据中心交换机一（单台）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| **＃**整机性能 | 交换容量≥390Gbps；  转发性能≥290Mpps；  整机包缓存≥3GB |
| 物理规格 | ≤2U标准机架式，配套上架配件 |
| **＃**端口 | 配置10/100/1000Base-T以太网端口≥96个， 1G/10G SFP+端口≥10个，万兆多模光纤模块（LC接口）≥2个 |
| 电源和风扇 | 配置模块化冗余电源、风扇 |
| **＃**虚拟化 | 支持跨设备链路聚合，单一IP管理，虚拟化后所有设备路由表项统一 |
| 支持通过标准以太端口进行堆叠 |
| 支持远程堆叠≥10km |
| VLAN特性 | 1、支持基于端口、协议、MAC的VLAN；  2、最大VLAN数(不是VLAN ID)≥4094；  3、支持802.1P，DSCP/TOS优先级和重新标记能力，支持基于时间段的流分类和QoS控制能力；  4、支持出方向的流量限速功能（Egress Car）；  提供广播风暴抑制功能； |
| 路由协议 | 1、支持IPv4静态路由、RIP V1/V2、OSPF、BGP、IS-IS;  2、支持IPv6静态路由、RIPng、OSPFv3、BGP4+、IS-IS V6  3、支持IPv4和IPv6环境下的策略路由  4、支持IPv6手动隧道、6to4隧道和ISATAP隧道 |
| 安全特性 | 支持802.1x认证，支持集中式MAC地址认证； |
| 支持IP+MAC+PORT的绑定； |
| 支持DHCP Snooping，防止欺骗的DHCP服务器； |
| 管理和维护 | 支持SNMP V1/V2/V3、RMON、SSHV2 |

### 数据中心交换机二（单台）

| **指标项** | **指标要求** |
| --- | --- |
| **＃**整机性能 | 背板带宽≥2.5Tbps；  包转发率≥1080Mpps |
| 物理规格 | ≤2U标准机架式，配套上架配件  可扩展槽位≥2个 |
| **＃**端口 | 配置万兆光端口≥48个，40GE端口≥6个, 万兆多模光模块300米(SFP+,LC)≥10个，  ,千兆多模光模块300米(SFP,LC)≥10个；  支持USB接口，支持带外管理接口 |
| 电源和风扇 | 配置模块化冗余电源、风扇 |
| 路由协议 | 支持静态路由、RIP v1/2、OSPF、BGP等动态路由协议，支持RIPng、OSPF V3、IS-IS V6、BGP+ FOR IPV6、IPV6策略路由，支持VRRP，支持等价路由 |
| VLAN | 支持基于端口/MAC/协议的VLAN；  支持最大VLAN数≥4094  支持QINQ及灵活QINQ |
| **＃**数据中心特性 | 实配支持VXLAN 二层/三层网关 |
| 支持OpenFlow+Netconf的VXLAN集中式控制平面，提供证明材料 |
| SDN/OPENFLOW | 提供可定义能力，支持netconf 、python、OPENFLOW 1.3  标准 |
| 支持普通模式和Openflow 模式切换 |
| 支持多控制器及SDN controller集群特性 |
| 支持多表流水线 |
| FCoE/FC特性 | 支持NPV或 Fip Snooping代理模式转发 |
| 支持FCF模式转发 |
| 支持VSAN的创建及配置 |
| 支持对端口接收报文的速率和发送报文的速率进行限制，限速粒度≤8Kbit/s |
| QOS能力 | 支持报文的802.1p和DSCP优先级重新标记 |
| 每端口支持的输出队列数≥8 |
| 支持PIM-DM、PIM-SM、IGMP、IGMP Snooping等组播协议；支持MLD，MLD Snooping、IPV6 PIM-DM、IPV6 PIM-SM 等IPv6组播协议 |
| 组播管理 | 支持SNMP V1/V2/V3；SSHv2；支持WEB网管，支持电源的告警功能 |
| 网络管理 | 支持风扇、温度告警 |
| 支持sFlow流量管理 |
| 支持IP+MAC+PORT的绑定； |
| 安全管理 | 支持DHCP Snooping，防止欺骗的DHCP服务器； |
| 支持黑洞MAC、动态ARP检测、ARP防攻击 |
| 提供工信部入网证和检验报告，提供复印件加盖厂商公章 |

### 汇聚交换机（单台）

| **指标项** | **参数要求** |
| --- | --- |
| **＃**整机性能 | 背板带宽≥2.5Tbps；  包转发率≥1400Mpps |
| 物理规格 | ≤2U标准机架式，配套上架配件 |
| **＃**地址表容量 | 整机最大MAC地址表≥280K |
| **＃**端口要求 | ≥24个万兆光端口（SFP+），≥24个万兆多模SFP+光模块（LC），配置模块化冗余电源，模块化冗余风扇。 |
| 扩展要求 | 整机最大万兆端口≥96，40GE端口≥8；  支持USB接口，支持带外管理接口；  扩展槽位≥4个。 |
| 交换协议 | 支持静态路由、RIP v1/2、OSPF、BGP等动态路由协议，支持RIPng、OSPF V3、IS-IS V6、BGP+ FOR IPV6、IPV6策略路由，支持VRRP，支持等价路由 |
| VLAN | 支持基于端口/MAC/协议的VLAN； |
| 支持最大VLAN数≥4094 |
| 支持QINQ及灵活QINQ |
| **＃**数据中心特性 | 实配支持VXLAN 二层/三层网关 |
| 支持OpenFlow+Netconf的VXLAN集中式控制平面 |
| SDN/OPENFLOW | 提供可定义能力，支持netconf 、python、OPENFLOW 1.3标准 |
| 支持普通模式和Openflow 模式切换 |
| 支持多控制器及SDN controller集群特性 |
| 支持多表流水线 |
| QOS能力 | 支持对端口接收报文的速率和发送报文的速率进行限制，限速粒度≤8Kbit/s |
| 支持报文的802.1p和DSCP优先级重新标记 |
| 每端口支持的输出队列数≥8 |
| 网络管理 | 支持SNMP V1/V2/V3；SSHv2；支持WEB网管，支持电源的告警功能 |
| 支持风扇、温度告警 |
| 支持sFlow流量管理 |
| 安全管理 | 支持IP+MAC+PORT的绑定； |
| 支持DHCP Snooping，防止欺骗的DHCP服务器； |
| 支持黑洞MAC、动态ARP检测、ARP防攻击 |

### 接入层交换机（单台）

| **指标项** | **指标要求** |
| --- | --- |
| **＃**设备性能 | 交换容量≥590Gbps，转发性能≥250Mpps |
| **＃**端口要求 | ≥48个GE端口，≥4个万兆SFP+端口 ，≥3个万兆多模光模块（LC接口），配置堆叠模块、堆叠线缆（每两台配置一条堆叠线缆），配置模块化冗余电源，模块化冗余风扇。 |
| 端口扩展性 | 最大可支持SFP+端口数量≥12，支持扩展40G端口 |
| 虚拟化 | 支持跨设备链路聚合，单一IP管理，虚拟化后所有设备路由表项统一 |
| 支持通过标准以太端口进行堆叠 |
| 支持远程堆叠≥10km |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 最大VLAN数(不是VLAN ID)≥4094 |
| **＃**数据中心特性 | 支持VXLAN 二层交换 |
| 支持VXLAN 路由交换 |
| 支持VXLAN 网关 |
| 支持OpenFlow+Netconf的VxLAN集中式控制平面 |
| SDN/OPENFLOW | 支持OpenFlow 1.3标准 |
| 支持多控制器（EQUAL模式、主备模式） |
| 支持多表流水线 |
| QOS | 每端口支持8个优先级队列； |
| 支持802.1P，DSCP/TOS优先级和重新标记能力，支持基于时间段的流分类和QoS控制能力； |
| 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF、BGP、等价路由、策略路由 |
| 支持IPv6静态路由、RIPng、OSPFv3、BGP4+ |
| 支持IPv4和IPv6环境下的策略路由 |
| 支持IPv6手动隧道、6to4隧道和ISATAP隧道 |
| 访问控制策略 | 支持基于第二层、第三层和第四层的ACL； |
| 整机提供ACl条目数不小于6K条； |
| 支持IPv6 ACL； |
| 支持出方向ACL，以便于灵活实现数据包过滤； |
| **＃**有线无线一体化 | 内置软AC功能，交换平台实现有线无线一体化 |
| 安全特性 | 支持802.1x认证，支持集中式MAC地址认证； |
| 支持IP+MAC+PORT的绑定； |
| 支持DHCP Snooping，防止欺骗的DHCP服务器； |
| 硬件板卡 | 支持扩展防火墙、入网防御、负载均衡插卡， |

### 存储光纤交换机一（单台）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| **＃**配置要求 | ≥24个16GB端口，≥24端口激活授权  提供≥24\*16Gb多模SFP模块；  冗余电源、冗余风扇  配套上架附件 |

### 存储光纤交换机二（单台）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| **＃**配置要求 | ≥24个8Gb端口,≥8端口激活授权；  提供≥8\*8Gb多模SFP模块；  配套上架附件 |

### POE交换机（单台）

| **功能指标** | **参数要求** |
| --- | --- |
| **＃**设备性能 | 交换容量≥598Gbps，转发性能≥210Mpps |
| **＃**端口要求 | 1、配置千兆电口≥24个，千兆光口≥4个；  2、配置热插拔内置双电源、内置双风扇； |
| 接口扩展 | 最大可支持万兆接口数量≥12 |
| 支持扩展40G端口 |
| 虚拟化 | 支持跨设备链路聚合，单一IP管理，虚拟化后所有设备路由表项统一 |
| 支持通过标准以太端口进行堆叠 |
| 支持远程堆叠≥10km |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 最大VLAN数(不是VLAN ID)≥4094 |
| **＃**数据中心特性 | 支持VXLAN 二层交换、路由交换、网关；  支持OpenFlow+Netconf的VxLAN集中式控制平面 |
| SDN/OPENFLOW | 支持OpenFlow 1.3标准 |
| 支持多控制器（EQUAL模式、主备模式） |
| 支持多表流水线 |
| 路由协议 | 支持静态路由、RIP V1/V2、OSPF、BGP、等价路由、策略路由 |
| 访问控制策略 | 支持基于第二层、第三层和第四层的ACL； |
| 整机提供ACl条目数不小于6K条； |
| 支持IPv6 ACL； |
| 支持出方向ACL，以便于灵活实现数据包过滤； |
| **＃**有线无线一体化 | 内置软AC功能，交换平台实现有线无线一体化 |
| POE供电能力 | 要求支持POE与POE+两种供电方式，所有电口均可POE供电，最大POE供电功率≥700W |
| 安全特性 | 支持802.1x认证，支持集中式MAC地址认证； |
| 支持IP+MAC+PORT的绑定； |
| 支持DHCP Snooping，防止欺骗的DHCP服务器； |
| 硬件板卡 | 支持扩展防火墙、入网防御、负载均衡插卡， |

### 万兆防火墙（单台）

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 架构 | 多核AMP+架构，标准2U机箱，冗余电源 |
| **＃**端口要求 | 配置多模SFP+万兆接口≥8个，300米多模SFP+模块≥8个；  配置多模SFP千兆接口≥4个，多模SFP千兆模块≥4个；  10/100/1000M Base-TX接口≥4个；  扩展槽位≥4个；管理网口≥1个；HA接口≥1个；串口≥1个 |
| **＃**性能要求 | 网络层最大吞吐量≥30Gbps；  应用层吞吐量≥12Gbps；  网络层并发连接数≥400万，每秒新建连接数≥28万 |
| **＃**功能许可 | 通过授权方式可在线扩展URL过滤、病毒防护功能、VPN、入侵防御模块、app应用识别等功能 |
| 网络适应性 | 1、具备多模式的网络部署方式和路由转发功能；  2、上行端口和下行端口可以支持联动功能，以适应在多机多链路接入时，可以进行智能链路检查和切换；  3、须支持服务器负载均衡，要求支持轮流、权重轮流、最少连接、加权最少连接等算法，采用≥2种方法主动探测服务器的存活状态; |
| 防火墙 | 支持详尽细化的会话超时时间自定义设置，包括：TCP握手、TCP建立、TCP单向关闭、关闭、UDP单向数据、UDP的DNS、UDP的其他、其他协议、GRE协议、TCP长连接、UDP长连接和其他协议的长连接 |
| 支持基于地理区域的安全策略及地理区域对象的导入 |
| 支持会话限制功能，可以根据IP地址、安全域（入、出、双向）、应用对单个IP或所有IP进行新建和并发连接限制  支持按源目的IP、源目的接口、用户、地理区域及应用进行流量排名，并显示流量统计 |
| 虚拟防火墙 | 支持虚拟系统并支持虚系统接口，用来实现虚拟系统间通信，可对每台虚拟系统自由分配系统资源，支持对每台虚拟系统进行独立管理 |
| 支持攻击防护、黑名单和入侵防御功能、路由、交换、监控、审计、安全、防护等全隔离，支持虚系统配置、日志及监控统计的独立管理 |
| 支持虚拟二层安全域、虚拟三层安全域，支持构建虚系统来实现与管理业务的分组与隔离，以及各个虚系统防护策略的可定制化 |
| URL过滤 | 预置≥86类URL资源库，可离线或在线进行更新升级，支持自定义URL条目，支持URL云查询 |
| 入侵防护 | 入侵防护功能开启。  支持对应用层Flood攻击进行五种处理动作：警告、阻断、普通防护、增强防护及授权服务器防护，支持TC反弹技术和ns重定向技术，支持SYN Cookie设置； |
| 支持局域网广播防护，支持全局配置的局域网广播防护及基于二层接口的局域网广播防护； |
| 支持DHCP防护，具备DHCP服务器检查、DHCP请求检查和DHCP请求限速等功能； |
| 支持对应用层Flood攻击进行五种处理动作：警告、阻断、普通防护、增强防护及授权服务器防护，支持TC反弹技术和ns重定向技术，支持SYN Cookie设置；  支持实时的入侵防护事件分级报警列表，可按事件的源IP、目的IP、协议、时间等显示；通过不同的入侵防护事件实时阻断入侵源IP，阻断时间可控。 |
| WEB安全 | WEB安全模块开启。  基于安全云的威胁防护与系统联动，支持与未知威胁感知系统联动来对用户网络进行文件分析、行为分析和病毒分析，可针对各种已知或未知威胁进行感知预警，并将可疑的名单发送给防火墙，防火墙依据名单动态生成策略，并根据用户配置决定这些可疑地址穿过防火墙时，执行拒绝或告警等防护动作； |
| 支持与终端安全管理系统联动，可通过搜集分析用户终端产生流量、进程及应用信息等，统一传递至防火墙后再提交安全云中心，由云中心对应用进行检测识别，记录相关信息；扫描检测存在的已知或未知的病毒、0day漏洞、未知恶意代码和APT攻击等信息。然后将所有信息传递至防火墙，动态生成对应的应用管控策略或木马查杀策略 |
| 防病毒 | 防病毒模块开启。  支持病毒云查杀，提供全面、强劲的病毒检测及防护功能 |
| 管理配置 | 支持自定义管理权限，包括模块：系统、网路、路由、对象、安全、VPN、PKI、用户认证、行为管理、应用安全、日志、监控、账户、虚系统；  支持特征库在线升级，支持指定升级服务器和代理服务器；  多系统设置可在Web界面上完成全部操作； |
| 统一认证集中管理 | 可通过与入侵防护、防弱口令扫描、未知威胁感知系统、终端安全管理系统的联动，生成动态策略信息，命中动态策略的数据将会被阻断或者记录日志；  支持终端安全管理系统协同联动，支持根据不同级别设置动作的情报配置，支持基于协议、本地地址、本地端口、本地证书、状态的情报接收，支持基于协议、远端地址、远端端口、URL地址状态的情报查询 |
| 高可用性 | 支持抢占模式和非抢占模式，并支持非抢占模式强制主备切换，支持透明模式非对称主主部署；  支持多系统引导，并可通过WEB界面配置启动顺序，要求具备恢复系统，并支持独立的完整备份；  配置、会话、用户状态可以在高可用性模式下进行同步 |

### 安全网关（单台）

| **指标项** | **招标要求** |
| --- | --- |
| 硬件要求 | ≤15U，机框式插卡设备，采用控制、数据、业务相分离的全分布式架构，配置双主控引擎； |
| 支持冗余交流电源，本次实配电源数≥6个； |
| 板卡槽位数≥8； |
| **＃**配置  要求 | 1、设备须支持配置防火墙、入侵防护、Web应用防火墙、负载均衡、上网行为管理、SSL VPN等应用层面或安全层面的功能的硬件板卡  2、≥24个千兆光口，≥48个10/100/1000 M以太网电口，≥34个万兆SPF+接口，≥20个万兆多模光模块  3、配置双主控引擎、≥4个交换网板、≥4个交流电源模块 |
| **＃**整机性能 | 吞吐量≥40Tbps；包转发率≥15000Mpps； |
| 防火墙板卡 | 须配置防火墙硬件板卡，特征库升级需≥5年。  吞吐量≥20Gbps；并发连接数≥800万；新建并发数≥12万；  硬件要求：实配12个千兆电口、12个千兆光口（所有接口非复用口 |
| 入侵防护板卡 | 须配置入侵防护硬件板卡，特征库升级需≥5年。  吞吐量：6Gbps；并发连接数：800万；新建并发数：10万；  硬件要求：实配12个千兆电口、12个千兆光口（所有接口非复用口 |
| 基本功能 | 1、支持IPv4、IPv6静态路由、等价路由、策略路由，以及BGP、RIPv2、OSPF、ISIS等动态IPv4路由协议，支持BGP4+、OSPFv3、ISISV6等动态IPv6路由协议  2、支持Web认证，支持MAC认证，支持AAA/Radius，支持SSHv1.5/SSHv2  3、支持动态划分VLAN；支持静态VLAN和802.1Q VLAN Trunk；VLAN数≥4K  4、具备并配置二、三层MPLS VPN；支持分布式 MPLS VPN处理；  5、支持跨设备链路聚合，允许多台物理设备完成虚拟化之后，不同物理设备的物理端口合并成一个逻辑端口  6、支持源地址NAT转换、目的地址NAT(nat server)、支持静态NAT映射、支持Fullcone NAT、支持NAT二进制日志，可以设置发送开始、结束日志、活跃流日志 |
| 防火墙板卡功能要求 | **＃**1、支持安全集群，将多台物理设备虚拟化为1台逻辑设备来统一配置管理，提供集群配置截图。 |
| 2、支持虚拟防火墙，支持将1台设备虚拟化为多台设备使用，可为虚墙划分各类硬件资源(至少包括CPU、内存、存储空间)，支持网络虚拟化（如IP、VLAN、VRF资源） |
| 3、每单板虚拟防火墙≥256个 |
| 4、支持URL过滤，支持特征库自动升级/手动升级/回滚 |
| 5、支持对死亡之Ping、IP分片重叠攻击、UDP攻击、ICMP Smurf攻击、Tear Drop攻击的防护； |
| 入侵防护板卡功能要求 | 1、支持缺省策略、支持自定义策略  2、支持特征库手动、自动升级、支持预定义特征、支持自定义特征（可以通过snort文件导入自定义特征）  3、支持 阻断/丢弃/允许/断开/重定向/捕获/日志  4、支持重定向报文、支持单独或组合配置特征动作  5、支持对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件、DoS/DDoS等常见的攻击防御  6、支持缓冲区溢出、SQL注入、IDS/IPS逃逸等攻击的防御  7、支持攻击特征库的分类（根据攻击类型、目标机系统进行分类）、分级（分高、中、低、提示四级）  支持攻击特征库的手动和自动升级（TFTP和HTTP）  支持对BT等P2P/IM识别和控制 |
| 系统管理 | 支持中文管理界面  支持FTP、TFTP  支持WEB管理接口  支持SNMP v1/v2/v3  支持RMON  支持NTP时钟 |

### 堡垒机（单台）

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 规格要求 | ≤2U设备，采用专用硬件平台和安全操作系统，软硬件一体化 |
| 提供≥6个千兆电口，冗余电源，支持1个可扩展插槽，支持液晶屏显示：接口IP，以及CPU、内存、硬盘的使用率等 |
| **＃**性能要求 | 图形会话并发连接数≥200 |
| 字符会话并发连接数≥700 |
| **＃**授权许可 | ≥100 |
| 部署方式 | 物理旁路部署，支持双机热备（冷备、主主模式），支持分布式部署，可部署多台运维审计设备共同负载访问压力 |
| 设备访问方式 | Web访问方式：支持使用IE、360、谷歌、火狐等浏览器打开堡垒机页面直接调用Mstsc、SecureCRT、Xshell、Xftp、Winscp、FlashfXP等运维客户端工具 |
| 支持MAC登录，并兼容MAC自带safari浏览器、item等工具。 |
| 支持批量登录登录多台协议相同的目标设备 |
| FTP菜单登录方式：支持使用Filezilla、Xftp、 Winscp、FlashfXP等客户端工具登录堡垒机访问FTP服务器 |
| 支持Secure CRT、Xshell等通过rz/sz命令实现文件上传下载 |
| 密钥访问模式：支持堡垒机可生成密钥进行下载后放置服务器内，在单点登录时，直接输入账号即可实现单点登录操作 |
| AD域数字证书登录模式：通过AD与服务器生成数字证书导入堡垒机内，在单点登录时，直接输入账号即可实现单点登录操作 |
| 快速登录：支持RDP、SSH、Telnet等协议快速登录 |
| 支持协议类型 | 字符协议：SSH、Telnet |
| 图形协议：RDP、VNC、X11 |
| 文件传输协议：FTP、SFTP |
| 支持web应用发布 |
| 支持数据库客户端发布，如Oracle、MSSQL、MySQL、DB2等 |
| 支持第三方C/S、B/S客户端发布，如IE、Vsphere client、plsql developer 、Magic Winmail、Navicat等 |
| 用户管理功能 | 支持运维用户的全生命周期管理，包括添加、修改、删除、停用/启动、更新时间 |
| 支持用户角色划分，如系统管理员、资产管理员、审计员、密码保管员、操作员等， |
| 支持对用户进行分组管理 |
| 支持Excel表用户批量导入/导出 |
| 支持对用户按科室、部门等进行独立管理、独立授权 |
| 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 |
| 支持运维用户多次登录失败自动锁定账号功能 |
| 资源管理功能 | 支持主机管理，包括主机 IP、名称、类型、访问协议、端口、帐号及密码等信息 |
| 支持对主机设备进行分组管理 |
| 支持Excel表主机设备批量导入/导出 |
| 支持对主机设备按科室、部门等进行独立管理、独立授权 |
| 支持资产学习功能，快速添加网络中的资产 |
| 支持批量修改资源信息 |
| 支持主机帐户和密码的自动登录、手动登录、半自动登录模式 |
| 身份认证 | 堡垒机认证方式：本地认证、RADIUS 认证、LDAP 认证、AD 域认证 |
| 支持静态密码认证 |
| 支持USB Key认证，可联动北京CA、飞天诚信、国泰新点等证书 |
| 支持动态令牌认证 |
| 须内置Radius服务器用以联动手机令牌认证，手机端认证软件需支持Google [authentication](http://www.baidu.com/link?url=TbANQc372DDIy0wUsFiYvJvFgVsm2OmlE3us3G9ZeenLInL1kv1BkJvLfu7hM3EesJJOqSwOjRR7vnJHcEI7Q1uRseQghRrcJFIZM5ysSCEgYiiF8kd2bngRdfmq_fEl)、FreeOTP。 |
| 支持联动短信网关认证 |
| 支持双因素认证 |
| 支持证书认证 |
| 访问策略及异常告警 | 支持通过基于时间、IP/IP段、用户/用户组、目标设备/设备组、设备账号、协议类型等组合访问控制策略，授权用户可访问的目标设备 |
| 支持时间集管理，支持基于时间集配置访问控制策略 |
| 支持IP集管理，支持基于IP集配置访问控制策略 |
| 支持对违规或高危指令拦截，支持指令黑白名单 |
| 支持临时授权审批：对资源临时访问需经过管理员审核后方可进行 |
| 支持指令审批：对资源执行关机、重启等重要指令需经过管理员审核后方可执行 |
| 支持二次审批：对敏感资产的操作需经过管理员审核后方可进行 |
| 支持指令审批告警 |
| 支持对用户/用户组违规操作告警 |
| 支持邮件方式告警 |
| 自动改密管理 | 支持定期自动修改Windows、Linux/Unix、网络设备、安全设备、数据库等目标设备密码功能 |
| 支持基于目标设备/设备组、密码复杂度、改密周期等配置自动改密策略 |
| 支持发送改密通知，发送方式支持邮件、FTP等 |
| 支持生成密码信封文件，并联动密码打印机打印出银行级信封密件 |
| 支持密码信封文件导出，信封文件支持txt、excel、zip三种格式，信封文件加密保护 |
| 需支持密码校验机制：保存新、旧两份密码，在设备改密出现异常时，可以通过登录校验，确认目标设备的正确密码； |
| 系统修改密码后，支持自动进行新密码登录测试。 |
| 操作审计及检索 | 支持对字符协议、图形协议、数据库操作进行记录 |
| 支持文件操作记录，如对文件的上传、下载、删除、修改等操作记录 |
| 支持对SSH的sz/rz命令、zmodem协议传输的原始文件完整记录 |
| 支持对FTP/SFTP传输的原始文件完整记录 |
| 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 |
| 支持全局搜索，通过关键字直接定位，无需区分图形/字符/文件/应用类型 |
| 支持上传文本内容记录，可对bat等可执行、内容不可见的批处理文件内容进行完整审 |
| 支持特殊按键记录，可以审计到右键、中键、左键等鼠标操作 |
| 支持视频日志删除功能，定期删除过期日志，保证磁盘空间充足 |
| 操作回放 | 支持审计日志视频回放，无需另外安装播放软件 |
| 支持倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作 |
| 支持回放界面中显示键盘输入、特殊按键 |
| 支持协议回放空闲时间过滤，支持应用发布图像回放空闲过滤 |
| 支持视频日志导出至FTP/SFTP服务器功能 |
| 支持视频日志离线播放，日志文件由专用播放器打开 |
| 实时监控 | 系统状态监控：支持堡垒机自身状态监控，包括 CPU、内存、磁盘的运行/使用情况 |
| 审计系统监控：支持记录审计系统自身的管理操作，保障自身安全 |
| 支持对RDP、VNC、Telnet、SSH等协议会话进行实时监控,实时监控功能要求“无延迟”，监控画面与操作画面之间的延迟不得超过0.5秒。 |
| 支持对实时监控的会话手动阻断 |
| 审计报表 | 支持以html、Excel、txt、word、csv、pdf方式生成并导出报表 |
| 系统自带报表模板 |
| 支持以多种图形方式（柱形图、饼图、折线图等）展示报表内容 |
| 支持根据用户实际需求，定制报表内容及格式 |
| 支持按日、周、月自动生成报表，并发送至制定邮箱 |
| 系统管理功能 | 支持NTP时间同步 |
| 重启堡垒机的操作只能使用密钥登录到堡垒机console菜单执行，在WEB页面关机、重启堡垒机的操作风险较高。支持 WEB 页面实现对堡垒机的关机、重启 |
| 支持超出CPU、内存、磁盘预设阀值产生告警 |
| 支持WEB页面IP配置、静态路由配置 |
| 支持WEB页面syslog、snmp配置 |

### 网络准入网关（单台）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 性能及部署要求 | 单台支持2000个用户数的并发 |
| 硬件支持至少6个千兆电口 |
| ≥1.5Gbps的数据吞吐率，≥100万并发连接数，最大新建连接数≥16000个/S |
| 单台至少支持4路业务控制 |
| 设备要求支持支持串接和旁路部署模式 |
| 注册管理 | 支持自定义注册信息，根据需要启用/禁用自定义项。 |
| 要求可根据需要自定义客户端注册的服务端地址，客户端可自动识别服务端信息并注册。 |
| 支持针对IE、弹出窗口等web形式的访问提供入网重定向提示，提示进行客户端注册，提示内容支持自定义修改。 |
| 要求支持注册审核管理功能，已注册终端必须通过管理员手动审核通过之后才可以接入网络。 |
| 身份认证 | 要求支持未认证通过用户入网时进行阻断，能够提供Web重定向提醒，并说明入网阻断原因。 |
| 要求支持与Radius认证系统联动进行身份认证，必须支持包含PAP、EAP-MD5、MD5-CHAP等加密认证方式。支持单账号、多账号认证。 |
| 支持与AD域服务器、LDAP服务器实现联动认证，并且支持帐户信息的自动同步；支持与CA认证系统联动实现身份认证。 |
| 要求支持基于终端心跳和终端水印认证双重准入判断，能够发现采用NAT模式入网的终端并强制认证。 |
| 要求支持认证日志记录和查询功能，应支持五个以上查询条件组合进行查询。 |
| 访客控制 | 要求支持外来终端或者访客初次入网阻断，并给出入网指导提示 |
| 要求支持外来终端或者访客自助申请上网码。 |
| 要求支持访客上网码短信审核功能。 |
| 系统监控 | 要求支持对在线终端状态提供图形化实时分析报表。 |
| 要求支持对系统本身业务接口的连接状态以及接口速率进行监控，支持对系统本身的CPU以及内存使用率提供仪表盘式图形化实时监控数据。 |
| 系统安全 | **＃**产品采用自主研发的专业实时操作系统，系统内核应该专为准入控制功能设计，不基于任何现有公用操作系统平台（例如：windiows、linux、unix）。 |
| 要求设备提供内置旁路模块，设备异常时切换到Bypass模式。 |
| 系统管理 | 要求支持基于https的B/S架构管理、支持基于SSH的命令行操作管理界面、支持基于serial串口的设备后台管理模式 |
| 支持邮件或者短信告警机制，支持与短信网关联动。 |
| **#**系统兼容Intel vPro主动管理技术。（提供功能截图证明） |
| 支持OEM自定义功能，提供OEM设置接口，管理员可随意更换页面LOGO以满足自身要求。 |

### 应用负载均衡（单台）

| **指标项** | **招标要求** |
| --- | --- |
| 性能参数 | 千兆端口≥10，万兆端口≥2； |
| 独立专业负载设备，X86架构，非插卡式扩展的设备； |
| 最大并发连接≥5,000,000；四层处理能力≥75 K CPS；最大SSL TPS 2K Key≥2000； |
| 内存≥8GB； |
| 最大压缩性能≥2.5Gbps；背板带宽≥56Gbps； |
| **＃**吞吐量≥10Gbps；七层处理能力≥212K RPS；  最大SSL加密吞吐量≥4Gbps； |
| 配置4核CPU, 支持多核CPU并行处理技术； |
| 存储硬盘≥500GB； |
| 系统冗余 | 支持Active-Active及Active-standby冗余方式；提供专用的硬件心跳线和网络级冗余判断方式；提供连接会话的镜像功能，实现无缝故障切换。 |
|  | 1、管理界面提供基于某种编程语言（如TCL语言）自定义的流量控制方法，免费提供可以和设备联动的厂商编程工具，支持语法检查和代码高亮显示。 |
|  | 2、支持在线升级功能，并支持基于Web的升级方式。 |
| 系统要求 | 3、支持多台设备基于同一网段和不同网段的N+M集群方式，同一集群中的设备支持不同平台，包括硬件平台和虚拟化平台。 |
|  | **#**4、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。声明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。 |
|  | 5、提供基于设备运行事件的可编程自动运维系统，支持将收集数据自动FTP上传或发送告警邮件。 |
|  | 1、内置SSL加速芯片。 |
|  | 2、支持将一个用户的多个请求或者多个用户的请求合成一个连接发送到服务器。 |
|  | 3、利用内存来缓存用户频繁访问的web动态和静态内容。 |
|  | 4、四/七层带宽管理和流量整形(Qos)：通过优先级，队列，以及设定基于应用的带宽限制和带宽容许，确保关键应用能够按时交付。 |
|  | 5、完善的第四/七层交换功能，支持可定制的基于应用层的健康检查方式，支持基于IP地址、Cookie等信息的会话保持，并可根据特定信息定制会话保持方式。 |
| 应用交付要求 | **＃**6、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。 |
|  | **＃**7、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。提供证明材料 |
|  | 8、内置全球地址IP地址库，可以识别访问者IP地址的所在国家，省份，运营商等信息。基于这些信息可提供更精准的访问分配策略及访问日志。 |
|  | 9、支持实时漏洞检测功能，通过对实时流量进行安全性分析来评估业务系统的漏洞风险，结合黑客攻击行为进行关联分析，帮助用户找到真正存在高风险的安全薄弱环节，并通过报表的方式展现安全风险和解决方法。 |
|  | 1、提供免费的在线自助巡检系统，生成状态诊断和分析报告。 |
| 管理要求 | 2、应用性能监控：管理界面可直接提供应用访问的网络延时和服务器延时、TOP URL、以及各虚拟服务器的CPU、内存等资源的占用比。 |
|  | 4、无需利用端口镜向功能，系统自身提供的类似tcpdump的实时抓包和分析工具。 |

### 数据库审计（单台）

| **指标项** | **招标要求** |
| --- | --- |
| 配置要求 | 2U上架设备，1个100/1000M Base-Tx管理口，≥2个100/1000M Base-Tx监控口；  ≥8G内存；  ≥2T硬盘； |
| **#**性能要求 | ≥峰值20000条SQL/秒级吞吐量  ≥400万/小时入库速率  ≥4亿条在线SQL语句存储支持  ≥140亿条归档SQL语句存储支持  支持大数据平台部署 |
| 支持≥5个数据库 |
| 支持国际主流数据库Oracle、SQL Server、MySQL、DB2、Postgres、sybase、informix、cacheDB等，国产数据库DM、GBase、KingBase等； |
| 基本审计能力和策略 | 1、审计内容包括：会话的终端信息、会话的主机信息、数据库名、登录时间、会话时长、操作信息、操作影响范围信息。  2、包含where、who、what、when、how、oter的审计过滤规则。  3、应用关联审计：能以完全精确方式，审计到应用端相关信息。  **#**4、支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小, 提供证明材料。  5、支持Weblogic、tomcat、Websphere、Jboss等主流的应用服务器。  6、支持与堡垒主机自动关联审计通过ssh、rdp等加密协议操作数据库行为。  **#7、**支持对数据库自动建模及智能对异常行为告警功能；  8、支持耗时长、执行频繁的异常语句识别  9、支持活跃会话识别  10、支持失败登陆审计；  11、支持口令猜测，基于频次判断失败登录风险；  12、支持SQl语句模板化归类，基于语句模板关联客户端信息自定义风险语句、信任语句和不审计语句类型； |
| 安全防护能力 | 1、能对基于数据库漏洞进行攻击行为监测和告警，默认支持400个以上的数据库漏洞攻击规则库。  2、对以下高危行为，可自动识别并进行风险处理、告警通知：  批量数据导出、高危操作（对超过特定行数阀值的批量数据修改、删除，或全表Update、Delete行为等）；新型语句的识别；SQL注入行为的识别  3、基于数据库设置，从优先级和规则类别两个层面创建并查询审计规则；  4、、风险操作支持多条规则逻辑关联，根据排列顺序区分优先级；  5、支持SQL注入监测：根据IP，sql特征和正则表达式自定义SQL注入  6、支持数据库漏洞监测和审计语句统一管理。 |
| 审计结果展现与查询 | 1、三个纬度的导航：会话维度、风险纬度、SQL分布  2、操作记录的信息：审计结果中包括：告警级别、事件发生时间、客户端IP、目标数据库IP、操作类型、客户端MAC地址、客户端端口号、返回状态、结果信息、客户端执行命令等详细信息内容。  3、支持基于时间、IP地址、数据库服务器IP地址、用户名、数据库操作命令、数据库表名，执行结果，应用用户等多种丰富的查询检索条件。  4、风险分析：根据敏感语句、sql注入、漏洞攻击、风险操作等维度以时间维度统计数据库分信息。支持规则命中查询、支持风险检索。  5、语句分析：基于SQL语句的操作类型统计，支持失败sql统计、Top sql统计；支持针对新型语句、语句审计模板检索。  6、提供图表结合的展形式，支持柱状图、饼状图、折线图等多种展示方式；  7、提供（系统级）多数据库聚合报表展现和单数据库综合性报表展现。  8、基于总体概况、性能、会话、语句、风险多层面展现报表。  9、支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式。  10、支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义敏感数据掩码规则11、支持报表定时推动功能，自定义推送周期以邮件形式推送报表文档。  12、支持日、周、月 等综合性报表和自定义分析型报表功能。  13、报表文档格式：WORD\ PDF |
| 告警和阻断策略 | 1、支持敏感语句告警策略。自定义添加敏感语句和信任语句，根据风险操作、SQL注入、漏洞攻击检测、语句管理等模块定义告警规则  2、支持高、中、低风险告警。  3、支持系统资源监控与告警。  4、告警方式包括：邮件、短信、SYSLOG、SNMP  5、系统内置独立的故障排错系统，可以支持一键导出加密的系统调试日志，支持一键检测服务、许可证、流量等大部分常见常见故障的检测（提供功能截图证明） |
| 网络部署 | 1、在旁路部署模式下，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。  2、支持数据库自动发现。设备无需添加、即插即用。 |

### 入侵监控软件（单套）

| **指标项** | **招标要求** |
| --- | --- |
| 基本功能 | 对自身进程、配置文件、服务等进行保护，防止进程被非法注入、接口被恶意调用；  具备掉线及时通知，并具备一定的自恢复功能；  可以通过B/S管理方式对所有主机进行集中管理。 |
| 安装时不影响正常业务运转，无需重启服务或系统，安装流程应简洁快速，单台服务器安装时间不应超过三分钟。 |
| 可以自动感知系统中主机和操作系统分布和监控系统覆盖情况，持续清点主机的IP、上线时段、状态，以及操作系统的发行、内核版本等信息。 |
| 安全防护 | 1、可以清点服务器上的系统账号情况，实时掌握系统账号信息。  2、可以清点业务主机上已部署的软件应用。  3、可以清点所有服务器上正在运行的内外Web站点，Web站点对应的端口、服务类型、运行权限、目录位置、目录权限、目录所有者信息等。  4、可以清点Web服务器上部署的第三方Web应用。  5、可以清点Web服务器上所有CGI接口，监控Web接口中的上传接口、登录接口、敏感信息接口等。  6、可以精准分析系统及软件漏洞，包括漏洞发现、影响范围、修复建议等。支持对漏洞进行多维度的筛选如有无POC等，其中漏洞修复建议应具体到批处理命令。  7、可以精准分析与发现常见Web应用漏洞。  8、可以对高风险文件如配置文件、脚本文件、日志、数据文件等进行自动监控，预防渗透或泄露事件。  9、可以深度有效地检测整个业务系统的各个层级的弱口令，需支持主动式探测分析与被动识别和捕获。  10、可以对当前主机系统的基线进行统一检查，实时列出检查结果，检查项应可灵活调整，根据自身需求灵活定制。  11、可以对黑客行为如账号组ID设置、黑客工具下载、数据外传、网卡混杂模式等进行全面的监控。  12、可以进行多层次webshell识别，支持自定义规则集，支持沙盒分析，外部联动。  13、可以精确发现反弹shell的情况。  14、支持实时邮件告警。 |

### 内网文件管控系统（单套）

| **指标项** | **招标要求** |
| --- | --- |
| 品牌 | 一体化设备，非OEM产品 |
| 配置要求 | 1、3U机架式一体化设备，配置≥16盘位设备，存储容量48TB；  2、配置64位6核处理器，64G高速缓存；  3、配置四个千兆网口；  4、支持目标段主流的32位和64位系统，配置≥200个客户端授权许可。 |
| 系统要求 | 1、桌面数据一体化保护设备基于存储专用的64位UNIX嵌入式系统，不接受Windows或Linux内核，存储系统及软件功能预装在独立的存储介质中，不占用RAID硬盘组的存储空间 |
| **＃**2、支持通用RAID 0、1、5、6、50、60等多种RAID方式，同时要求具备三重奇偶校验技术 ，支持任意三块硬盘同时损坏数据不丢, 提供管理界面截图。  3、能够实现存储参数信息、RAID信息、介质信息的自动导出，当存储设备系统介质故障，可采用新介质更替，原有的存储参数信息、RAID信息、介质信息可采用导入操作，原有信息不丢失，充分保障设备安全性；因故障风险条件，不接受RAID1方式, 提供管理界面截图。 |
| 权限管理 | 系统管理员以Web方式登陆管理系统，提供权限功能，权限身份分为：高级管理员，组管理员，审计员，组成员；高级管理员后台可设置文件强制保护策略 |
| 文件管控 | 1、设备具备桌面级文件管控功能，支持集中式，强制性的文件实时保护，在保护过程中，无需人工干预；  2、支持自定义目录、自定义文件类型、自定义文件名称等多种保护策略；  3、在保护过程中支持断点续传功能 |
| **#**1、支持桌面级的文件恢复，包括整个逻辑卷、单个目录、或单个文件的细粒度恢复；支持选择某一历史时间点的恢复，可恢复到该文件的某个历史状态；并采用旁路设计，在部署时或系统故障时不影响业务系统正常运行；在恢复过程中，支持断点续传功能,提供证明材料。  2、支持数据的在线预览，保障业务连续性；支持已保护文件针对其关键字进行检索；支持一键数据本地恢复功能；  3、支持系统资源智能调节功能，包括三个级别：智能均衡，性能优先和速度优先等，最大程度提高资源利用率； |
| 文件共享 | **＃**1、设备包含文件共享功能，个人用户可将文件数据上传到共享空间，并有权将文件共享给某组或某组的组成员；  2、设备包含个人网盘功能，并支持共享网盘的容量配额，管理员可针对用户组、用户分别进行配额管理。  3、设备支持个人网盘隔离功能，当设备内存在多个用户的个人网盘时，每个个人网盘是一个独立的文件系统，并非所有网盘共在一个文件系统下，当存在多个网盘用户时，即存在多个平行的文件系统。 |

### 协议分析仪（单套）

| **指标项** | **招标要求** |
| --- | --- |
| 基本要求 | 支持全中文界面和资料文档  支持中英文双语解码  旁路方式部署在网络中，不能改变网络原有的结构  要求该系统能够支持10M/100M/1000M以太网环境 |
| 硬件要求 | 采集口：千兆电口数量≥2个；  千兆光口数量≥2个  管理口：千兆电口数量≥2个 |
| 性能要求 | 1、支持每秒流量捕捉能力大于4Gbps；  2、支持每秒捕获数据包120000个；  3、数据包捕获的时间分析精度达到微秒级；  4、支持420种及以上网络协议识别及解码分析。 |
| 部署要求 | 1、要求能够支持流量镜像、分路器等方式部署。  能够实现链路聚合功能，能将多网卡的流量聚合捕获分析。  2、支持多任务分析，能够针对某网络接口支持多个捕获和分析任务同时进行分析。  3、捕获数据包时能够根据条件过滤捕获。 |
| 功能要求 | 1、通过捕获底层数据包，能得到数据在每层的原始数据。支持多任务的分析。支持对网络攻击行为、安全隐患进行直观的分析，并对事件能快速准确的定位。支持定时分析功能。 |
| 2、支持根据不同的网络按不同配置进行分析，包括对数据采集方式，过滤器，分析模块、解码模块等进行配置。 |
| 3. 实时监控特定IP的通讯流量信息刷新频率为1秒，提供证明截图。 |
| **＃**4、支持自定义报表统计。支持报警。支持对单台主机的tcp同步包发送数量和接收数量进行监控和告警。支持对主机的应用交易处理数量进行监控和告警。支持对主机的ip会话数量和TCP/UDP会话数量进行监控和告警。支持多种数据包格式的导入导出，包括：\*.cscpkt、\*.cap、\*.pkt、\*.rawpk、\*.dmp，提供证明材料。 |
| 5、支持对所有节点（MAC，IP）进行矩阵查看。支持数据回放。支持实时分析网络数据。支持报文编辑并发送数据包。支持自定义协议。支持自定义图表，能够对网络流量进行实时图形化展现。支持日志功能，包括DNS、Email、FTP、HTTP、MSN、Yahoo；支持日志导出CSV、LOG格式。支持工程全局配置信息导入导出。 |
| **＃**6、支持物理地址和IP 地址的别名+地址组合显示。支持TCP协议分析及数据流重组。支持ARP地址解析协议分析。支持邮件协议POP3、SMTP协议分析。支持ICMP协议报文分析。支持FTP协议报文分析。支持DNS、RTP协议报文分析。支持HTTP协协议报文分析，提供界面截图。 |
| 7、支持MAC地址扫描。支持网络分析档案。支持会话交互视图。支持数据包视图增加高亮和备注。各视图支持显示过滤功能，提供证明材料。 |
| 安全分析 | 1、支持自动判断存在ARP攻击行为的主机并在单独的分析视图中展现。  2、支持自动判断存在DOS攻击的主机的网络行为特征并在单独的分析视图中展现。  3、支持自动判断存在TCP端口扫描的主机的网络行为特征并在单独的分析视图中展现。  4、支持自动判断存在可疑的HTTP、POP3、SMTP会话的主机的网络行为特征并在单独的分析视图中展现。  5、支持自动判断存在感染蠕虫病毒的主机的网络行为特征并在单独的分析视图中展现。 |

### 邮件防火墙（单台）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 规格 | 1U 或 2U 机架式 |
| 配置 | 至少配有一颗64位Intel 至强 4核处理器，主频≥2.2GHz |
| 内存≥8G；磁盘有效存贮空间≥1TB，且必须支持RAID技术；至少有一个1Gigabit以太口 |
| 基本功能 | 有效邮件用户数：≥15000；邮件域数量：≥1500 |
| 邮件日志容量：≥124GB；隔离区容量：≥160GB |
| 支持外发邮件过滤；支持邮件加密；支持syslog |
| 支持多语种过滤，至少支持简繁中文、英文以及识别多语言编码； |
| 支持判断邮件虚拟发件人及虚拟邮件路由并对伪造的电子邮件限制发送； |
| 支持用户自定义信头、主题、信体关键字过滤功能，能设置阻断、隔离、标记和白名单，关键字的泛定义支持Perl正则表达式； |
| 支持用户自定义IP黑白名单、发件人域黑白名单、发件人黑白名单、收件人黑白名单功能； |
| 可根据规则扫描和隔离相关类型附件（包括压缩文件），附件文件格式可自定义。 |
| 支持发件人特征识别技术； |
| 支持基于规则的评分系统过滤技术，规则库包含中文简繁字符规则，规则库支持自动更新； |
| 支持意图分析过滤技术，能识别最新图形化的垃圾邮件。 |
| 支持邮件指纹过滤技术；支持SPF技术 |
| 支持并抵御各类针对邮件服务系统的DDOS攻击、暴力破解密码攻击等攻击行为； |
| 支持SMTP及LDAP邮件认证功能 |
| 支持与微软AD集成的SSO，包括LDAP，POP，RADIUS登录认证 |
| 支持远程IMAP/POP账号过滤 |
| 备份功能 | 管理功能支持用户分层分级权限设置；  支持对邮件用户进行垃圾邮件扫描、邮件隔离以及垃圾邮件自主评分等功能的开启或关闭； |

### 杀毒软件（单套）

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 基本要求 | 国产品牌 |
| **#**防病毒终端数量≥1500个，服务器端≥终端数500个 |
| 系统管理 | 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；  客户端：与安全控制中心通信，提供控制中心管理所需的相关数据信息；执行最终的木马病毒查杀、漏洞修复等安全操作；  产品支持终端保护密码；  支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告；  支持自定义默认分组的终端默认功能模块,包括产品功能模块及实用工具等；  支持控制中心数据恢复与备份； |
| 病毒、恶意代码、木马防护 | 要求产品本身具备病毒检测功能，并且通过CheckMark、ICSA、OPSWAT等各大国际评测机构联合认证； |
| 要求产品具备本地多引擎查杀能力，且引擎可配置。 |
| 要求产品具备公有云检测能力，并且公有云特征储备超过100亿。 |
| 支持私有云查杀，预置至少2亿黑名单及2000万全面的白名单，终端威胁统一到控制中心查询黑白并进行查杀。 |
| 内存实时监控查毒，能够自动隔离感染而暂时无法修复的文件 |
| #支持linux、国产操作系统杀毒、云桌面（至少两家）产品 |
| #要求产品在断网状态下具备不依赖病毒库特征的情况下对未知病毒查杀的能力，提供专利证明材料。 |
| #要求产品具备主动防御技术及相关发明专利 |
| 要求产品具备应用级沙箱技术。 |
| 按病毒、木马显示展示全网涉及的终端，可查杀指定或全部木马、加入信任；按终端显示展示全网每个终端存在的病毒、木马及可查杀的 |
| 要求支持对网内未知文件云查询的控制，可以选择直接连接互联网云查询中心查询，也可以选择采用私有云查杀引擎完成未知文件查询。 |
| 要求支持以自定义黑白名单的方式来管理全网终端的文件。管理员可以将文件加入白名单或者黑名单。 |
| 要求支持通过数字签名或者文件名的方式分别显示文件 |
| 要求上报文件至少包括:文件名称、发现时间、鉴定结果、文件大小、数字签名和文件所属源计算机等信息 |
| 要求能够支持漏洞利用防御，尤其对通过文件漏洞（尤其是0day漏洞）的攻击行为进行有效检测与防御。 |
| 支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置 |
| 要求支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力。 |
| 对敲诈者病毒提供防护机制，同时提供解密工具，解密工具应为自主研发。 |
| 病毒库升级管理 | 要求支持服务器端病毒库的定时更新和手动更新两种升级模式；  要求支持客户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽。 |
| 补丁分发与漏洞修复 | 要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型； |
| 支持漏洞修复影响文档编辑时提醒功能； |
| 支持补丁下载安装顺序设置 |
| 支持自定义补丁排除名单 |
| **#**终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，提供截图。 |
| **#**产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能 |
| **#**要求产品生产公司具备热补丁修复功能 |
| **#**要求产品生产公司具备面向微软官方级别漏洞发现能力，提供证明材料 |
| 产品具备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 |
| 服务器端功能 | 支持服务器、PC、虚拟化的同台管理；  至少支持Windows Server 2003、2008、2012 三个版本操作系统平台的杀毒防护与漏洞管理，并可对Windows xp 和Windows Server 2003提供后续漏洞防护；  至少支持3个以上Linux服务器版本并且可以和Windows统一管理；  如果未来服务器端采用虚拟化技术进行业务升级，需要提供配套的解决方案用于服务器虚拟化的安全防护； |
| 资产管理 | 按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控CPU温度、硬盘温度和主板温度 |
| 支持终端软、硬件变更审计，资产清单报表； |
| 支持统计指定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率 |
| 支持自动发现设备的IP-MAC地址的绑定 |
| 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 |
| **#**支持正版软件的正版序列号的读取功能，确保软件正版化。 |
| 支持远程协助终端、远程关机、重启终端 |
| 日志报表 | 展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表；展示全网终端病毒库日期比例； |
| 展示指定时间段内指定终端修复漏洞，病毒查杀，木马查杀的情况 |
| 要求支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人。 |
| **#**支持大数据引擎系统，可将全网终端日常运维数据汇聚存储分析，并根据客户运维管理所需的要求定制报表 |
| 运维管控 | 可统计指定终端网络、应用程序的上传，下载速度与流量； |
| 支持冗余有线网卡、无线网卡、3G网卡、MODEM、ADSL、ISDN等设备的外联控制；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 |
| 支持终端进程红名单、黑名单、白名单功能，可设置核心进程必须运行，也可保护核心进程不被结束。 |
| 支持网址黑、白名单；可设置终端不能访问的网址URL，终端访问这些URL时会被拦截，并展示拦截记录 |
| 支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限 |
| 支持对终端桌面系统的账号密码、本地安全策略、控制面板、屏保与壁纸、浏览器安全、杀毒软件检查 |
| 终端支持在线、离线两种策略，可同时使用在线或离线两种状态，保证终端安全运行。 |
| 移动存储介质管理 | 支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括学习注册、授权、启用、停用、删除、取消注册、导出注册列表等 |
| 支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批； |
| 支持移动存储介质读写权限划分设置，有效控制不明来历的移动存储可能带来的病毒传播等隐患 |
| **#**支持移动存储介质外出管理，并可以设置外出使用权限以及外出使用次数与有效时间； |
| 支持移动存储介质权限设为普通设备与加密设备，可设置是否允许网外使用； |
| **#**可提供硬件安全U盘与终端安全管理系统联动。 |
| 硬件安全U盘文件系统采用私有文件系统，可以有效防止剖片攻击。 |
| 硬件安全U盘在身份认证之前不能访问数据区密文。在身份认证过程中，存在口令尝试次数限制，可有效防止暴力破解。口令认证过程受安全芯片保护。 |
| 安全U盘日志记录文件的操作时间，登录账号，操作记录，使用U盘的计算机名，源文件路径，目标文件等信息日志存储受安全芯片保护，防止篡改。 |
| 硬件安全U盘的日志记录不受网络限制，脱离内网仍可进行操作审计 |
| 日志报表 | 记录安全U盘的文件操作时间，登录账号，操作记录，使用U盘的计算机名，源文件路径，目标文件等信息；  日志抓取不受内外网限制，会如实抓取用户的操作行为；  日志存储受安全芯片保护，防止篡改 |
| XP防护 | **#**支持针对Windows XP系统可带来安全隐患的设计机制进行加固性修复，至少支持10以上防护机制； |
| 支持Windows XP热补丁修复，公司拥有自己的热补丁引擎； |
| 支持安全沙箱技术，可对word、excel、ppt等程序进行沙箱隔离运行； |
| 支持系统IE降权，防止黑客利用IE浏览器提权渗透； |
| 终端审计 | 支持移动存储设备、网络共享服务器、本地硬盘特定扩展名或特定目录下的文件访问、修改、删除、移动等行为的审计 |
| 支持网络打印操作、本地打印操作、虚拟打印操作审计，记录包含终端ＩＰ，文件名称与类型，打印机名称，纸张类型等信息；支持自定义文档类型的打印审计； |
| 支持邮件发送审计，通过设置例外,忽略已知类型的可信邮箱,如本企业的内网或外网邮箱等,重点记录未知收件人的邮件日志； |
| 支持终端访问的互联网全日志的审计，支持自定义浏览器进程与主机地址的筛选； |
| 支持对应用程序的启动和停止进行记录,统计软件运行的活动状态 |
| 支持USB、蓝牙或红外等终端外设接口接入外设的使用情况审计 |
| 支持终端的启动、关闭、待机、休眠、等状态的记录与统计 |
| 支持本机账户或域账户登录日志统计 |
| 支持安全U盘操作日志的审计，支持离网使用日志审计 |
| 设备联动 | **#**支持与旁路威胁检测系统设备、NGFW、上网行为管理、VPN产品联动，达到网关边界联动防御效果 |
| 其他功能 | #功能模块包含：防病毒功能授权（Windows客户端）、Windows 客户端补丁管理功能授权、运维管控功能授权、终端审计功能授权，可以通过授权在线开通XP遁甲、移动存储，MAC OS X系统的病毒防护、数据价值评估功能授权、企业软件管家功能授权等功能，提供厂家授权免费开通功能声明。 |
| 终端准入 | 支持旁路终端准入部署方式，避免串行设备部署单点故障； 支持有线、无线基于应用协议准入方式，准入配置支持保护服务器区域、例外终端等灵活的配置方式； 支持标准802.1X准入，支持动态VLAN、动态ACL下发； |
| 支持哑终端设备入网控制； |
| **#**支持终端安全检查失败本地ACL隔离机制，可基于协议、特定端口、端口范围、特定地址、IP范围、URL来控制终端访问权限，从而无需操作交换机达到终端网络控制目的，实现细粒度的访问控制管理，支持不同终端修复区域定义。 |
| **#**支持802.1X认证技术上基于终端快速认证，与终端管理客户端联动无需输入账号快速入网，避免重复输入账号口令。 |
| **#**支持AD、LDAP、Email、HTTP、本地等多种方式认证源统一认证管理。 |
| 支持入网健康检查策略，策略检查项至少包括：远程桌面、U盘自动运行、防火墙、IP获取方式、文件共享、屏幕保护、空密码、IE代理；支持终端修复向导 |
| **#**配套服务 | 为招标方提供原杀毒软件卸载及新软件安装服务。 |
| **许可要求** | 杀毒软件授权许可为一年。 |

### 域名解析设备（单台）

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 兼容性 | 需与报社现ZDNS-T5100设备兼容 |
| 软件要求 | 专用DNS设备； |
| 硬件要求 | QPS：≥8万  存储空间：≥500G；  网口：≥8个10/100/1000M电口  双网卡支持互为主备和负载均衡方式  冗余双电源 |
| 管理 | **＃**云部署：必须支持内部域名服务系统的分层次分布式部署，集中管理，各节点数据统一下发，并能保证数据一致性。设备之间通信以密文进行传输。支持多地HA部署；能与报社现网内域名解析设备实现统一管理。 |
| **＃**可视化中文界面，支持多角色管理和授权 |
| 支持网络地图，实时显示现有节点信息，包括：网络信息、连接状态、地理位置等 |
| 支持设备分组，进行组内节点数据统一配置管理 |
| 提供web页面的软件系统“一键式”平台升降级服务，无需操作人员登陆设备底层进行命令行操作 |
| 支持灾难恢复机制，能够自动备份和恢复单个节点，支持解析记录的定时自动备份（可设定备份周期）和人工触发的数据备份 |
| 兼容性 | 支持IPv6、DNSSEC、DNS64、国际化域名IDNs等，支持IPv4和IPv6双栈等下一代互联网技术；  支持和微软AD域结合 |
| 技术要求 | 提供：DNS serverfail攻击安全防护、请求源地址切换功能和多链路的服务优选、抗DDOS和缓存攻击、A记录和ptr联动等功能 |
| 支持标准的递归和权威DNS功能 |
| 支持高性能DNS查询模式服务，并发性能不低于30万QPS。 |
| 可单独启用或停止递归功能; 支持递归请求失败跳转服务; 提供递归查询顺序转发服务; 支持基于视图的存根区、转发区和重定向; 支持多区多视图，支持资源记录的批量修改; 支持以ZONEFILE格式批量导入解析记录，支持增量导入; 支持共享记录 |
| 智能化的访问流量调度 |
| 支持应用服务器的健康检查 |
| 支持IP和域名的解析记录限速控制 |
| 支持辅区不过期、支持设置请求源地址和检查 |
| 支持对缓存记录的手动清除; 支持对DNS所有数据的全局搜索，模糊搜索; 支持DNS64和DNSSEC平滑部署; 支持TFTP服务; 支持时间同步 |
| 日志与告警 | 提供DNS解析、操作日志及统计报告功能，可根据日志的严重等级，实现定制化发送到多台LOG服务器；  要求支持中文图形化方式的全局所有子节点监控，  支持邮件、SNMP接口和URL回调等报警方式； |

### 高密度无线AP（单台）

| **指标项** | **指标要求** |
| --- | --- |
| 兼容性 | 可与现网H3C S10510无线控制器建立CAPWAP隧道，可以被现网网管系统管理 |
| 工作模式 | 可支持胖/瘦AP两种工作模式，采用整机八流设计，可同时工作在802.11a/b/g/n/ac/ac wave2模式。 |
| 协议支持 | 支持802.11a/n/ac和802.11b/g/n。 |
| 射频卡配置 | 要求投标产品提供三个射频模块设计。 |
| 部署模式 | 放装部署。 |
| 协商速率 | 5GHz单射频卡单终端协商速率支持1733Mbps，2.4GHz单射频卡单终端协商速率支持300Mbps，整机无线并发最高接入速率可达3000Mbps。 |
| MU-MIMO特性 | 须支持MU-MIMO特性，且MU-MIMO流数≥6 |
| 接口 | ≥2个10/100/1000Mbps(RJ45)，支持端口负载均衡 |
| 双网口均可进行PoE供电，单端口供电失败后，设备依然通过另外一个端口供电 |
| 天线 | 内置智能天线设计 |
| 工作温度 | 温度：-10~55度范围 |
| 工作湿度 | 湿度：5%~95% |
| 加密 | 支持64、128位WEP加密，WPA，802.11i和WAPI。 |
| 用户隔离 | 支持AP上二层转发抑制 |
| 支持虚拟AP(多SSID)之间的隔离 |
| SSID隐藏 | 支持 |
| 频谱导航 | 支持 |
| 配置要求 | 提供配套电源适配器及安装配件 |

### 蓝牙无线AP（单台）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 工作模式 | 1、支持胖/瘦AP两种工作模式, 支持802.11ac协议;  2、支持蓝牙4.0可管理iBeacon（包括但不限于设备参数显示、电量监测、推送内容下发）。 |
| 兼容性 | 可以与现网H3C S10510无线控制器建立CAPWAP隧道，可以被现网网管系统管理 |
| 协议支持 | 1、同时支持802.11a/n/ac和802.11b/g/n工作；  802.11ac/n/a:5.725GHz-5.850GHz; 5.15~5.35GHz (中国)  802.11b/g/n:2.4GHz-2.483GHz(中国), 2.4GHz/5GHz双频段同时工作,  以上工作频段要求与无线型号核准证上一致。  2、支持Bluetooth：2.402GHz-2.48GHz |
| 接口 | ≥1个10/100/1000Mbps(RJ45)以太网电接口 |
| 协商速率 | 5GHz支持866Mbps，2.4GHz支持300Mbps |
| 天线接口 | 内置天线 |
| 供电 | PoE或本地电源适配器 |
| IPv6支持 | 支持IPv4/IPv6双协议栈、Native原生，特别支持IPv6 Portal |
| 灵活转发 | 支持 |
| TR-069动态分支管理 | 支持 |
| 加密 | 支持64、128位WEP加密，WPA，802.11i和WAPI。 |
| 用户隔离 | 支持AP上二层转发抑制；  支持虚拟AP(多SSID)之间的隔离 |
| 报文过滤 | 支持 |
| 实时频谱防护 | 支持 |
| 802.11e | 支持 |
| QoS策略映射 | 支持不同SSID/VLAN映射不同的QoS策略 |
| 用户数负载均衡 | 支持 |
| 流量负载均衡 | 支持 |
| 智能带宽限速 | 1、基于带宽均分算法  2、基于每用户指定带宽的算法  3、在流量未拥塞时，确保不同优先级SSID下的报文都可以自由通过；在流量拥塞时，确保每个SSID可以保持各自约定的最小带宽 |
| 频谱导航 | 支持 |
| 组播转单播 | 支持 |
| 配置要求 | 提供配套iBeacon模块及iBeacon电量管理系统； |

### 无线面板AP（单台）

| **指标项** | **指标要求** |
| --- | --- |
| 工作模式 | 可支持胖/瘦AP两种工作模式，支持802.11ac Wave2协议，支持MU-MIMO； |
| 兼容性 | 可以与现网H3C S10510无线控制器建立CAPWAP隧道，可以被现网网管系统管理 |
| 协议支持 | 同时支持802.11a/n/ac/ac Wave2和802.11b/g/n工作 |
| 接口 | LAN接口≥4个10/100/1000Mbps以太网电接口；  WAN接口≥2个10/100/1000Mbps以太网电接口 |
| 接口要求 | 在设备断电状态下，可传输数据接口≥1个 |
| 特殊接口 | 标准USB接口≥1个 |
| 协商速率 | 5GHz: 866Mbps  2.4GHz:300Mbps |
| 天线 | 内置天线 |
| 供电 | 支持Poe供电，且支持本地电源适配器供电 |
| TR-069动态分支管理 | 支持 |
| 加密 | 支持64、128位WEP加密，WPA，802.11i和WAPI。 |
| 报文过滤 | 支持 |
| 实时频谱防护 | 支持 |
| wIPS 探针 | 支持 |
| SSID隐藏 | 支持 |
| MAC地址过滤 | 支持 |
| 802.11e | 支持 |
| QoS策略映射 | 支持不同SSID/VLAN映射不同的QoS策略 |
| 用户数负载均衡 | 支持 |
| 配置要求 | 提供安装配件 |

### 300M无线AP（单台）

| **指标项** | **指标要求** |
| --- | --- |
| 工作模式 | 可支持胖/瘦AP两种工作模式，支持802.11ac Wave2协议，支持MU-MIMO； |
| 兼容性 | 可以与现网H3C S10510无线控制器建立CAPWAP隧道，可以被现网网管系统管理 |
| 协议支持 | 同时支持802.11a/n/ac/ac Wave2和802.11b/g/n工作 |
| 接口 | ≥2个10/100/1000Mbps(RJ45)，双网口可冗余PoE供电、支持端口负载均衡。 |
| 功耗 | 整机最大功耗小于12.5W |
| USB接口扩展 | ≥1个USB扩展口 |
| 天线 | 内置天线 |
| 协商速率 | 5GHz频段867Mbps，2.4GHz频段400Mbps |
| 核准频段 | 802.11a/n/ac : 5.725GHz-5.850GHz (中国)  802.11b/g/n : 2.4GHz-2.483GHz (中国) |
| 供电 | 支持RJ45网线供电或本地电源适配器 |
| IPv6支持 | 支持IPv4/IPv6双协议栈、Native原生，特别支持IPv6 Portal、IPv6 SAVI |
| 灵活转发 | 支持 |
| TR-069动态分支管理 | 支持 |
| 实时频谱防护 | 支持 |
| 认证 | PORTAL认证(远程,外挂服务器)、基于SSID的Portal页面推送、基于AP的Portal页面推送、Portal支持代理功能、Portal双机热备、SSID防假冒(用户名与SSID绑定)、LDAP |
| 智能带宽限速 | 1、基于带宽均分算法  2、基于每用户指定带宽的算法  3、在流量未拥塞时，确保不同优先级SSID下的报文都可以自由通过；在流量拥塞时，确保每个SSID可以保持各自约定的最小带宽 |
| 配置要求 | 提供配套安装配件 |

### VPN设备（单台）

|  |  |
| --- | --- |
| 指标项 | 招标要求 |
| 硬件平台要求 | ≤1U设备，X86架构，配置≥6个千兆电口。 |
| 提供移动安全接入流量≥120M，支持并发人数≥800人。 |
| 授权要求 | 1、开启企业移动管理接入功能，提供≥300个工作域隔离授权；  2、SSL VPN接入授权≥300个；  3、开启远程应用发布接入模块，提供≥100授权。 |
| 企业移动管理(EMM)套件平台App封装加固 | 1、设备须支持SDK方式的App封装，支持Android和iOS版本；  2、支持针对移动应用（iOS和Android）App的安全代码的自动封装；  3、应用封装必须支持Per App安全隧道，支持应用图形锁，要求集成安全SDK的企业APP需具备手势认证功能，为企业应用的切换提供快速的二次验证机制。 |
| 企业移动管理(EMM)套件平台工作域隔离与应用管理 | 1、支持在Android、iOS终端上基于沙盒技术生成隔离的安全工作区域；  2、支持第三方移动App的自动封装，并发布到企业应用商店中；  3、支持对企业App新版本进行提醒；  4、支持管理员远程锁定/解锁设备，让违规及丢失手机无法使用应用；  5、设备应支持消息推送功能，管理员可将通知消息推送至用户终端；  6、设备应对失联进行自动化策略管理，一旦失联时间超过设置阀值，EMM平台应通知管理员，并对失联设备发送锁定、擦除等管控指令；  7、支持对设备截屏、拍照、录像、录音功能进行管控，避免因窃听类恶意应用植入手机造成信息泄密。  8、IOS切换到后台后界面模糊，防止未授权的偷窥导致信息泄漏。 |
| 基础接入特性 | 1、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EMM设备同样可实现EMM接入用户的多线路自动优选功能；  2、支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复；  3、支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式；  #4、支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度，提供配置界面截图和证明材料；  5、针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，支持共享流缓存功能，提供证明材料。 |
| 身份认证安全 | 1、设备支持Local DB 、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；  2、支持与基于PKI体系的第三方CA进行结合认证 ，可根据CA某字段将通过CA认证的用户自动映射到指定用户组，进行权限授权配置；支持CRL证书撤销列表；  3、单台EMM管控设备可扩展同时支持≥5套CA根证书 |
| 网络传输安全 | 1、支持智能终端通过移动安全接入，部分新发布智能终端如遇兼容性问题无法使用APP时，需要保障用户使用浏览器访问WEB版应用，为APP升级提供过渡时间。  2、支持断线重连自动技术，防止用户在弱无线信号网络环境下网络正常切换时安全接入会话断开造成的企业APP反复登录；  3、支持移动安全接入专线功能，可配置用户在接入同时，断开与Internet其他连接。 |
| **#**集成要求 | 本次采购的设备可以与本单位国外部署的虚拟专线设备组成集群，提供设计方案 |

### 盘柜（单套）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 兼容性 | 招标方已有型号emc cx4-240 DAE ，需扩展盘柜并与原存储系统的磁盘兼容 |
| 规格 | 磁盘阵列存储模块（DAE），含≥15个槽位，配置≥15块600G 15K存储系统磁盘 |

### 邮件归档系统（单套）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 兼容性 | 须与报社现网coremail邮件系统兼容 |
| 邮件备份 | 自动实时归档邮件，避免邮件信息误删 |
| 邮件检索 | 有效的邮件检索和准确定位。 |
| 邮件调阅 | 邮件还原管理功能，可以利用历史邮件作为资料储备。 |
| 邮件稽核 | 分配邮件查阅权限，对邮件内容的审查审计和行为操作可进行安全监察。 |
| 设定归档邮件范围 | 对邮件进行分级，可全局设定邮件重要性。 |
| 支持自定义归档邮件统计策略 | 支持按邮件类型、事件范围、在线状态等统计 |
| 邮件恢复 | 邮件丢失，归档系统可把邮件重新恢复到邮件服务器。 |
| 日志管理 | 支持监察日志查询报表导出 |
| 敏捷的邮件检索 | 可通过设定关键词及正则表达式，来对归档邮件的主题、正文、以及附件内容进行检索查找。检索结果中，敏感词可进行高亮显示 |
| 支持三权分立的归档管理模式 | 支持配置系统管理员、安全监察员、邮件审计员帐号 |
| 提供关键字预警授权 | 关键字授权可指定条件，当归档邮件触发指定预警条件时，自动转发或抄送到设定的审计预警邮箱 |
| 提供异常事件统计 | 包括记录外网登录IP，登录频率和批量邮件下载次数，支持设置这些异常事件的阈值，超出系统自动弹出预警提示 |

### 监控显示屏4K（单台）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| ★显示参数 | 屏幕尺寸：43英寸  屏幕分辨率：超高清4K（≥3840x2160）  屏幕比例：16：9  背光源：LED  垂直刷新率：23-80Hz  面板类型：IPS面板  响应时间：≤8ms  支持格式（高清）：≥2160p  水平视角（度）：≥178 |
| **指标项** | **指标要求** |
| 端口参数 | Display Port：≥2个  USB3.0接口：≥4个  HDMI接口：≥2个  内置扬声器：≥2个 |
| 功耗参数 | 电源：100-240VAC，50-60Hz  待机功率：≤0.5W |

### 监控工作站（单台）

| **指标项** | **指标要求** |
| --- | --- |
| 参数配置 | 同等或优于第六代英特尔酷睿i5－6500 CPU  内存：≥8GB DDR4  ≥256G SDD硬盘  ≥4G 独立显存  电源规格：≥600W 能够支持硬件后续升级接入额外的板载设备  显示比例：宽屏16：9 |
| ★支持显示器物理分辨率 | 不低于4个4k显示屏 |
| ★显卡接口 | DP/Min-DP ≥ 4 |
| 其它参数 | 扩展性：PCI-E×2、DIMI×4  网络接口：10/100/1000Mbps  支持无线局域网  耳机、麦克风二合一接口  光驱：16X DVDRW  摄像头像素：720p  三年原厂服务  正版Windows系统7或10 |

### 移动工作站（单台）

| **指标项** | **指标要求** |
| --- | --- |
| 参数配置 | CPU类型：同等或优于第六代英特尔酷睿i5－7200U处理器  内存：≥8GB DDR3L 1600  硬盘：≥256G SSD硬盘  显卡类型：≥2G 独立显存  屏幕规格：≥14英寸  显示比例：宽屏16：9  物理分辨率：1920×1080  屏幕类型：LED背光  内置蓝牙：蓝牙4.1  局域网：10/100/1000Mbps  支持无线局域网  耳机、麦克风二合一接口  显示端口：MiniDP/HDMI  摄像头像素：720p  支持指纹识别  续航时间：≥8小时  100-240V自适应交流电源适配器  操作系统 ：Windows 10系统 |

## 三、项目实施要求

（一）编制项目管理及施工组织方案

1．投标人应在投标书中提出满足项目需求的项目详细实施方案计划。

2．投标人应自备库房，按照招标方项目进展需求提供设备入场。

3.项目进行过程中，投标人必须每周提交工作总结报告及下周工作计划。

4.方案内容包括但不限于投标人对整个工程的：

1）项目实施的组织结构保障

➢投标人必须有详细项目管理组织架构、职员姓名、职务、职称，主要资历、经验及承担过的项目。

➢列明负责本项目的项目实施小组名单及职责。

2）施工组织方案

方案总体设计主要内容要求（但不限于下列要求）：

1）项目需求分析、方案设计

●项目实施的进度计划：对项目实施的各个阶段：工程设计阶段、设备订货阶段、工程实施准备阶段、系统建设阶段（包括系统安装调试、设备开箱验货、设备安装调试、设备安装、加电测试、设备调试配置、系统调试等）、系统验收阶段的进度作出详细的计划；

●关键分项项目的施工方案

2）项目实施管理、集成、调试与迁移交付

3） 项目组织机构人员配备及管理体系

●对项目实施中各阶段中投标人所要做的工作及保障措施做出详细安排；

4）项目质量保证措施和保障措施

●包含施工进度计划及保证措施和违约责任承诺等

●对可能出现的非计划因素干扰提出控制措施。

●劳动力、材料和设备投入计划及保证措施

●投标人须提出项目实施中的工程技术设计、设备采购、系统安装调试和项目售后服务的全过程质量管理及控制提出具体措施，并提出质量保障目标的承诺。

●投标人须严格参照采购方单位《项目生命周期信息安全管理规程》规范进行项目规划及实施。

5） 项目验收评审

●项目验收之前，应完成安全测评工作并完成相关整改工作，并提供项目安全测评报告。

●项目验收资料包含但不限于系统测试、实施方案及应急演练等文档交付。

#（二）投标方提供实施所必须的线缆（光纤、网线）、辅材、标签等材料，提供承诺函加盖公章。

## 四、技术支持与售后服务要求

1、投标人须提供所投设备五年原厂免费维保及软件升级。

2、投标人须提供所投产品原厂的部署、实施、调试及相关配置服务。

3、投标人须提供培训服务，具体要求见下方：

a.投标商须须根据操作人员类型的不同提供培训方案计划，培训方案详细具体且有针对性。该方案须由投标商及原厂联合完成，并在方案内体现；

b.培训方式须至少包括远程、现场等方式；

c.培训资料须至少包含电子、纸质等形式；

d.培训师须为原厂且工龄超五年以上的工程师；

e.培训内容须至少包含项目中涉及的软、硬件技术交流及操作培训；

f.培训课时须至少满足200小时或50次。

4、自项目验收之日起，投标人须提供5年免费维保服务。维保期内，须提供的如下服务内容：

a.维保期内协助进行软件补丁升级许可及硬件维修；

b.提供7\*24小时远程响应，5×10小时工程师现场问题处理，2小时内备件更换及应急服务；

c.投标人提供的免费维保包括但不限于以下内容和方式：电话咨询、电话技术支持、远程支持、现场支持等；

d.在维保期内服务商须按照中国日报社要求每月进行巡检，提交巡检报告及时发现解决问题；

e.在维保期内投标人须按照中国日报社要求在每年至少六次重大节假日和重大出报活动过程中提供驻场技术支持服务。

## 五、评分标准（包一）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 评标项目 | 项目指标 | 评分标准 | 分值 | 对应的投标格式 |
| 招标报价（30分） | 招标报价 | （1）满足招标文件需求、且投标报价最低的为评标基准价，其投标人的报价分为最高分30分；  （2）其他投标人的价格分值统一按照下列公式计算：  报价得分=(评标基准价／投标报价)×价格权值×100； | 0～30 |  |
| 客观分（42分） | 资质 | 投标人通过ISO 27001 信息安全管理体系认证得2分，否则得0分。  注：需提供证书复印件并加盖投标人公章。 | 0～2 |  |
| 投标人通过ISO 20000 IT服务管理体系认证得2分，否则得0分。  注：需提供证书复印件并加盖投标人公章。 | 0～2 |  |
| 投标人通过ITSS信息技术服务运行维护标准符合性认证得2分，否则得0分。  注：需提供证书复印件并加盖投标人公章。 | 0～2 |  |
| 标书质量 | 有目录索引、页码无错乱、标题、编号、正文、表格等排版规范得2分，每出现一个错误扣0.5分，扣完为止。 | 0～2 |  |
| 原厂商服务承诺函 | 投标人提供原厂商针对本项目产品的售后服务承诺函（包含客户名称、招标编号），全部产品均有提供得8分，每少一个扣2分，扣完为止。 | 0～8 |  |
| 实施与服务偏离情况 | 1.满足招标文件中实施及服务要求的全部指标得4分。  2. #号指标不满足招标文件技术要求的，每有1项减2分，扣完为止。  3. 一般技术指标（不带#号）不满足招标文件技术要求的，每有1项减1分，扣完为止。  4. 要求提供证明材料的指标项必须提供合格证明材料，否则按不满足认定。 | 0～4 |  |
| 技术参数偏离情况 | 1.满足招标文件硬件产品要求的全部技术指标得20分；  2. #号指标不满足招标文件技术要求的，每有1项减2分，有5项（含）以上不满足得分即为0分。  3. 一般技术指标（不带#号）不满足招标文件技术要求的，每有1项减1分，有10项（含）以上不满足得分即为0分。  4. 要求提供证明材料的指标项必须提供合格证明材料，否则按不满足认定。 | 0～20 |  |
| 投标人承诺的所投所有产品质保期 | 所投所有产品质保期高于招标文件要求，所有设备质保期多1年得1分，最多得2分。 | 0～2 |  |
| 主观分（28分） | 项目集成方案 | 项目管理方案科学合理、详细完整，项目组织协调周密，人员架构优秀，提供详细的时间进度计划安排、质量控制、文档设计，按照方案的全面性、科学性排名，第一名得4分，第二名得2分，第三名得1分，其余不得分。 | 0～4 |  |
| 所投产品先进性、成熟性 | 针对本次所投存储设备，提供统一的管理、运维方案和对应的管理平台，按照方案的成熟性、可操作性排名，第一名得3分，第二名得2分，第三名得1分，其余不得分。 | 0～3 |  |
| 针对本所投服务器产品，提供合理的安全防护和系统管理方案，包括但不限于管理软件。按照方案的成熟性、先进性排名，第一名得3分，第二名得2分，第三名得1分，其余不得分。 | 0～3 |  |
| 针对本次所投防病毒产品，提供完善的终端管理功能和管理方案，按照方案的全面性、科学性排名，第一名得3分，第二名得2分，第三名得1分，其余不得分。 | 0～3 |  |
| 运维服务方案 | 运维服务方案全面科学，涵盖流程、人员、内容、备品备件等角度设计，根据方案的全面性、专业性排名，第一名得4分，第二名得2-3分，第三名得1分，其余不得分。  。 | 0～4 |  |
| 数据管理与数据安全 | 所投服务器、存储等具备数据处理、存储的设备，应具备完善的数据管理和数据安全保障机制或功能，包括但不限于内存、硬盘等的容错机制，数据压缩、数据快照、数据容灾和数据克隆等机制或功能。按功能优劣，覆盖所投设备范围等排名，第一名3分，第二名2分，第三名1分，其余不得分。 | 0～3 |  |
| 许可与授权 | 提供服务器、存储、数据库审计、入侵监控软件、防病毒软件等设备和软件许可和授权清单，并提供原厂商加盖公章的授权说明函：  1、存储设备包括但不限于CPU授权许可、控制器容量授权许可、多路径软件许可、存储管理软件的授权许可等；  2、服务器包括系统管理软件、安全防护软件等；  3、安全设备、软件包括数据库类型、特征库、病毒库等。  可永久免费使用、可更新且无容量、协议等条件限制的，得3分；有条件使用的，按照总体使用成本排序，第一名得2分，第二名得1分，第三名得0.5分，其余不得分。对于未在清单中列出的付费许可，使用费用由中标方承担。 | 0～3 |  |
| 应急响应 | 书面承诺提供7×24小时技术支持和现场服务，在用户提出服务需求后，10分钟内必须响应，2小时以内到达用户现场，到达现场后2小时内必须解决故障。满足得2分，不满足本项得0分。  注：须提供承诺函并加盖投标人公章。 | 0～2 |  |
| 培训 | 培训方案设计详细、形式全面、差异化安排得当，完全满足招标文件要求得3分，其余得0-2分。 | 0～3 |  |